VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA PRÁVA

Počítačová kriminalita, její ekonomické, technické a právní příčiny a důsledky

Computer Crime, its Economical, Technical and Legal Causes and Consequences

Student: Bc. Martina Horutová

Vedoucí diplomové práce: JUDr. Bohuslav Halfar

Ostrava 2011

MÍSTOPŘÍSEŽNÉ PROHLÁŠENÍ

„Místopřísežně prohlašuji, že jsem celou diplomovou práci, včetně všech příloh, vypracoval(a) samostatně a uvedl(a) jsem veškerou použitou literaturu a další prameny.“

V Ostravě dne 18. dubna 2011

…….
Martina Horutová

PODĚKOVÁNÍ

Ráda bych na tomto místě poděkovala všem, kteří mi byli v mé práci nápomocni. Především vedoucímu mé diplomové práce JUDr. Bohuslavu Halfarovi za odborné vedení, poskytování rad a věcné připomínky.

Dále své rodině za vytvoření optimálních podmínek a za podporu během celého studia, jehož zakončením je tato práce.

V Ostravě dne 18. dubna 2011

…….
Martina Horutová

Obsah:

1 Úvod

Společnost, ve které žijeme, se s časem dynamicky mění. Nemůžeme srovnávat situace dnešní doby se situacemi, které se odehrály třeba jen před rokem, natož před mnoha desetiletími či staletími. S rozvojem společnosti se mění i schopnosti a předpoklady lidí. Na jedné straně jsou lidé, kteří si život zjednodušují, protože toho díky moderní technice již nemusí tolik umět a dokázat. Na straně druhé jsou lidé, kteří se snaží tohoto rozvoje využít ke svému obohacení, ať již mentálnímu či ekonomickému. O lidech z této druhé skupiny nemůžeme jednoduše říct, že dělají něco špatného, ačkoliv to tak velká část společnosti chápe, a to jen proto, že měli sílu a odhodlání obohatit se.

Asi nejpodstatnějším přínosem pro společnost je dlouhodobý a stálý rozvoj moderních informačních a komunikačních technologií, díky kterým je vše rychlejší a jednodušší. Dále se díky Internetu pomyslně zkracují vzdálenosti mezi lidmi, kteří dnes mohou být v kontaktu téměř kdykoliv a kdekoliv. Počítače používáme k práci, zábavě, odpočinku. Veřejné informace jsou nám stále k dispozici. Dá se říci, že v těchto ohledech přináší moderní technologie obrovskou pomoc. Musíme však dodat, že všechny tyto technologie mají původ ve vojenství a speciálních programech nejmocnějších vlád světa a proto není překvapující, že se tyto prostředky často využívají i takovým způsobem, který lidem nepomáhá, ale škodí jim. Jedná se o počítačovou kriminalitu, která je tématem mé diplomové práce.

Počítačová kriminalita nebo také kyber-kriminalita je druh protizákonného jednání, které je vedeno proti počítačům, za použití počítačů a k nim přidružených technických prostředků jako jsou počítačové sítě. Tento druh kriminality mohl samozřejmě vzniknout, jako všechny ostatní druhy, až v době, kdy to umožnil rozvoj techniky, které se přímo týká. V této práci se chci také zabývat jednáním, které není přímo protizákonné, ale jakkoliv napomáhá rozvoji počítačové kriminality.

Cílem mé diplomové práce je definovat pojem počítačová kriminalita a rozebrat jednotlivé typy počítačové kriminality, a to jak protiprávní jednání s využitím počítačů, tak i protiprávní jednání směřující proti počítači. Dále zaměřit se na příčiny a důsledky počítačové kriminality. Pokusím se zjistit, jakým způsobem přispívají návyky uživatelů počítačů k rozšiřování kyber-kriminality. Zabývat se budu také pachateli těchto činů, neboť si musíme uvědomit, že to nejsou obyčejní lidé, ale lidé v tomto oboru velmi vzdělaní, kterých není až tak mnoho, jak by se dalo očekávat. Zhodnotím situaci v kyberprostoru, aspekty, které dovolují rozmach počítačové kriminality a kroky, které

jsou podnikány, aby počítačovou kriminalitu potlačovaly a bojovaly s ní. Dále se zaměřím na specifikaci právní úpravy počítačové kriminality a na závěr se pokusím navrhnout prevenční a represivní opatření, která by mohla vést k omezení počítačové kriminality.

Je třeba si uvědomit, že útočník je zpravidla vždy o krok napřed. Pak bývá jen otázkou, kolik dostane prostoru pro svou činnost, jak rychle bezpečnostní složky zareagují a do jaké míry jsou schopny mu jeho jednání zkomplikovat. Už z těchto několika důvodů bych netvrdila, že útočné jednání rozvoj společnosti brzdí. Spíše bych řekla, že musí zákonitě docházet k rychlejšímu rozvoji počítačových a komunikačních technologií především z hlediska bezpečnosti.

2 Historický vývoj počítačové kriminality a její právní úprava

2.1 Historický vývoj počítačové kriminality

Pro představu, jaká dnes počítačová kriminalita je a co znamená, je velmi důležité nejdříve poznat a pochopit, jak tato činnost vlastně vznikla a s čím souvisí. Proto další část věnuji historii počítačové kriminality a rozboru jejích jednotlivých částí.

Pro tuto práci si zvolím členění jednotlivých etap podle publikace Michala Matějky:[1]

1. Období od vynálezu telefonu po uvedení prvního PC na trh v roce 1981 značíme za ***pravěk***.
2. Období od roku 1981 do případu Citibank v roce 1994 označíme jako ***středověk***.
3. Období od roku 1994 dodnes budeme nazývat ***novověkem*** počítačové kriminality.

2.1.1 Pravěk

V době do roku 1981 se nedá mluvit o masovém rozšíření kriminality s využitím počítačů, protože jejich množství bylo zanedbatelné a možnost využití minimální. Tyto první počítače byly velmi drahé a také velmi hlídané, proto k nim mělo přístup jen několik programátorů. V této době však vzniklo slovo *hacker*, jakožto programátor, který si upravuje programy tak, aby fungovaly lépe a rychleji (zásahům do programu se říkalo *hacks*). Je nutno dodat, že nelegálnímu používání počítačů předcházelo, především v sedmdesátých letech dvacátého století, zneužívání telefonních linek (označuje se *phreaking*). Jednalo se především o vynalézání způsobů, jakými obelstít telefonní přístroje, ústředny a spoje tak, aby bylo možno telefonovat pokud možno zadarmo. Po propojení počítačů telefonními linkami se tento trend rozmohl směrem k počítačům.

S rozšířením kotoučových magnetofonových pásek můžeme hovořit o počátcích *porušování autorských práv*, neboť právě tato technologie umožnila kopírování hudby uživatelům v domácích podmínkách. I počítače používaly magnetofonové pásky jako záznamové médium a tak se tento druh kriminality ještě více zdokonalil s rozšiřováním Internetu. V této době již můžeme hovořit o masovém porušování autorských práv.

[1] MATĚJKA, M. *Počítačová kriminalita*. Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 17

Později, v 70. letech, se možnosti kopírování, především hudby, ještě o krok zjednodušily s příchodem kazetových magnetofonů. V době příchodu prvních PC (Personal Computer) se začalo rozmáhat nedovolené kopírování, distribuce a prodej počítačových programů.

2.1.2 Středověk

V roce 1981, přesněji 12. srpna, byl světu poprvé představen počítač typu IBM PC. Příchod tohoto stroje přinesl opravdovou revoluci v používání počítačů a také v pojímání kriminality kyber prostoru, nehledě na to, že se počítače pomocí modemů začaly propojovat do sítí a daly tak základ nejen Internetu, ale i možnosti způsobit vzdáleně škody jinému uživateli.

Nesmíme zapomenout na význam vytvoření prvních BBS (Bulletin Board System), které se staly skutečnými předchůdci Internetu. Tyto systémy umožňovaly vzájemnou komunikaci uživatelů, většinou počítačových nadšenců, předávání informací a také sdílení souborů. K velkému rozmachu používání BBS přispěl film „Wargames“ v roce 1983, který byl prvním filmem z hackerského prostředí. Toto dílo, ač velmi naivní a nereálné, ukazuje hackerskou činnost jako něco vzrušujícího a podbízí tak v divákovi touhu, aby zažil něco podobného jako hlavní hrdina.

V 80. letech vzniká také hackerská skupina Legion of Doom. Její členové začali po BBS šířit své samizdaty s názvem LoD Technical Journal. Jeden hacker z této skupiny způsobil v roce 1989 incident, který vyústil v první rozsáhlou policejní akci proti hackerům, nazvanou Sundevil. Operaci předcházelo vypracování žalob proti několika členům LoD a v rámci akce bylo zabaveno 42 počítačových serverů s BBS. Styl provedení tohoto zásahu vedl k velmi rozšířenému názoru, že celá akce měla mít spíše odstrašující charakter, a proto se začala naskýtat otázka řešení občanských svobod a svobody projevu v kyber prostoru. Další případ, o kterém stojí za to se zmínit, nese název Grateful Dead. V tomto případě šlo o krádež kódu firmy Apple Macintosh. Kódem byl ovladač výstupního zobrazení na monitor. Hackeři tento kód ukradli a rozeslali konkurentům firmy Apple. V souvislosti s tímto činem se FBI zaměřila také na člena rockové hudební kapely Grateful Dead Johna Barlowa. Ten byl aktivním členem hackerské konference, která však sdružovala hackery v původním smyslu slova. I přesto zabavila policie několika členům této skupiny počítač a tak se rozběhla ještě vášnivější diskuse na téma ochrany uživatelů počítačů. Jako největší problém viděli tito počítačoví odborníci a nadšenci fakt, že

počítačová policie bere všechny znalce moderních informačních technologií jako hrozbu. Proto John Barlow, společně s Michaelem Kaporem, společně založili Electronic frontier foundation - EFF (Nadace elektronického pohraničí), jejímž hlavním posláním je ochrana světa počítačů před nežádoucím vstupováním státní moci. Jejími prostředky k boji se stal lobbing, soudní spory a publicita. Nadace EFF funguje dodnes, jejím předsedou je John Buckman a John Barlow je členem představenstva.

Jako reakce na založení EFF vznikl na druhé straně FCIC, což byl spolek všech bezpečnostních složek USA, která má za úkol bojovat s počítačovou kriminalitou a jejími pachateli.

Za konec středověku ve vnímání historického vývoje počítačové kriminality považujeme okamžik, kdy se zásadně změnila povaha počítačového zločince. Nyní jím už není počítačový nadšenec, pro nějž představuje průnik do cizích systémů pouze výzvu, ale profesionální zločinci, kteří se snaží za použití moderních technologií obohatit obvykle o peníze.

Na počátku 90. let došlo k dalším dvěma případům, které rozjitřily další diskusi o počítačové kriminalitě. Jedná se o případ *Orchard Finger-Hackers* z roku 1993 a *Citibank* z roku 1994. V prvním případě se jednalo o podvodníky, kteří si vydělávali tím, že prodávali ukradená přístupová hesla pro telefonní spojení ilegálním imigrantům v New Yorku. V druhém případě se hlavními aktéry stala skupina hackerů vedených rusem Vladimírem Levinem. Tito hackeři pronikli do počítačů Citibank a odtud převedli na své účty deset milionů dolarů.

Výčet hackerů doby středověku však musíme doplnit o další tři jména. Prvním z nich je Kevin Mitnick, který se v roce 1988 naboural do počítačů společnosti Digital Equipment. Tento hacker se stal prvním pachatelem počítačového zločinu, který se objevil v seznamu FBI Most Wanted (nejhledanější zločinci na světě). Dalším slavným jménem v historii počítačové kriminality je Robert Morris. Ten vypustil do prostředí Internetu jednoho z prvních počítačových červů. Jako jméno červa je uváděno *Morris Worm* nebo *Internet Worm*. Podle jeho tvůrce nebyl program určen ke způsobení škod, ale k změření rozsáhlosti Internetu. Díky kritické chybě v systému šíření červa však došlo k prudkému napadení typu DoS (Denial of Service). Místo toho, aby se červ kopíroval pouze na dosud nenapadené stanice, začal se replikovat i na stanicích, kde byl již přítomen. Zajímavostí může být, že disketa s kódem červa, kterého Morris vytvořil, je uschována v Bostonském vědeckém muzeu. Za tyto přečiny si Kevin Mitnick odpykal rok ve vězení. Robet Morris pak zaplatil 10 000 dolarů a musel odpracovat větší počet hodin veřejně prospěšných prací.

Třetím jménem ve výčtu slavných hackerů je Kevin Poulsen. Pod přezdívkou *Dark Dante* se proslavil nabouráním se do telefonních linek jedné z rozhlasových stanic, kde „zařídil“, aby se dovolal jako 102. v pořadí a vyhrál tak Porsche 944 S2. Tento kousek ho stál 4 roky vězení a 58 000 dolarů. K tomuto trestu byl připojen tříletý zákaz práce s počítačem.

Dalším odvětvím počítačové kriminality, které se začalo v této době rozvíjet, je pirátství neboli útoky proti autorskému právu, týkajícího se jak počítačových programů, tak audio, video souborů a v dnešní době již i elektronických knih (e-books).

Tento skokový pokrok, co se pirátství týče, byl způsoben nově používaným médiem pro přenos dat-kompaktním diskem nebo CD, které umožňovalo kvalitnější zápis dat v tehdy, relativně, velkých množstvích. Toto médium se nejdříve používalo v polovině 80. let jako hudební disk a asi o půl desetiletí později se, s příchodem CD-ROM[2] mechaniky, začalo používat také k distribuci počítačových programů a her. Z počátku bylo nedovolené kopírování prakticky znemožněno velkými náklady, které by musel pachatel vydat na pořízení přístrojů, které by umožňovaly záznam na toto digitální médium. To se změnilo v polovině 90. let, kdy byly distribuovány první CD mechaniky umožňující zaznamenávat[3] data na CD. Tento počin je jedním z významných mezníků počítačové kriminality.

2.1.3 Novověk

Pro toto období je nejtypičtější masové rozšíření osobních počítačů, většinou s operačním systémem Microsoft Windows. S růstem počtu počítačů se pochopitelně rozšiřuje i trh s počítačovým softwarem, sítě typu Internet i Intranet. Do prostředí počítačů vstupují soukromé subjekty za účelem podnikání, Internet se komercializuje a přitékají do něj peníze. Tento stav samozřejmě přitahuje podvodníky, kteří se ho snaží využít ve svůj prospěch. Charakter pachatelů se mění z čirých nadšenců na profesionální zločince, kteří se zajímají pouze o svůj prospěch. Překvapením je fakt, že vliv tradiční mafie není v prostředí Internetu, tak výrazný, jak se očekávalo. Proto se protizákonné aktivity v prostředí počítačů omezují na úzce vyhrazené oblasti činností. Mezi tyto oblasti můžeme zařadit útoky na interní systémy bank, nebo zneužívání ukradených platebních karet. Vedle očekávání ovládnutí prostředí Internetu mafiemi vyslovili analytici další domněnku. Podle tohoto odhadu se měly stát moderní informační technologie nebezpečně účinným nástrojem v rukou teroristů na celém světě. Ani tento dohad se prozatím nestal skutečností,

[2]Počítačová mechanika pro čtení CD (CD-ROM – compact disc read only memory)
[3] také „vypalovat“ – odtud název „vypalovačka“

ačkoliv nikdy nemůžeme se stoprocentní jistotou říci, že teroristé moderní technologie při uskutečnění svých plánů nevyužijí. Prozatím jim minimálně otevírají cesty k jednoduššímu výzkumu a vývoji na poli biologických a chemických zbraní, získávání tajných informací, komunikace, apod. V této souvislosti můžeme mluvit o tzv. kyberterorismu, pod kterým si nemůžeme představovat typickou teroristickou činnosti. Spíše jsou jím zaštítěny nejběžnější a nejzávažnější trestné činy související s informačními technologiemi.

Období po roce 1994 je již velmi těžké rozdělit do dalších časových úseků. Proto bych se nyní, podle vzoru Matějky, ráda zmínila o mezníčích, které nám mohou toto časové období více přiblížit.

- ***Argentinský hacker (1995)***

V tomto případě se jednalo o činnost argentinského hackera, který zneužil počítačů na harvardské univerzitě k odposlechu provozu a zjišťování hesel pro přístup do vládních systémů. V souvislosti s pátráním po útočníkovi bylo soudem poprvé dovoleno odposlouchávání provozu v síti Internet policií.

- ***Případ Procesor Intel (1996)***

Bývalý zaměstnanec firmy Intel Guillermo Gaede se pokusil prodat výrobní tajemství týkající se procesoru Intel 486 konkurenční firmě AMD (Advanced Micro Devices). AMD však celý případ oznámila firmě Intel a ta podnikla kroky k potrestání svého zaměstnance. Pokud by plány byly skutečně prodány, mohl si Gaede přijít podle odhadů na částku mezi deseti a dvaceti miliony dolarů. Místo peněz bylo však Gaedemu přisouzeno strávit patnáct let ve vězení a navíc musel zaplatit pokutu ve výši pětiset tisíc dolarů. Nárok na podání žádosti o podmínečném propuštění vznikl po třiatřiceti měsících strávených za mřížemi.[4]

- ***Kontroverzní zákony USA týkající se informačních technologií (1996, 1998)***

V roce 1996 byl v USA přijat zákon, který stanovoval omezení pro obsah elektronické komunikace. Stanovoval pravomoci vládních orgánů a trestní odpovědnost osobám, které by na Internetu zveřejňovaly nezákonný obsah. Po přijetí zákona byla

[4] Findarticles. *Business Publications.* [online]. 23. 3. 1996 [cit. 23.01.2011]. Dostupný z WWW: <http://findarticles.com/p/articles/mi_m0EKF/is_n2109_v42/ai_18135525/>

okamžitě vytvořena hromadná žaloba proti platnosti tohoto zákona, pod kterou se podepsalo asi 10 000 subjektů včetně Microsoftu. Jako reakce na žalobu byly nepřípustné pasáže zákona 13. června 1996 zrušeny.

V roce 1998 byl přijat další ze zákonů upravujících podmínky používání moderních informačních a komunikačních technologií týkající se ochrany autorských práv. Tento zákon byl kontroverzní zejména tím, že ještě více do hloubky omezoval uživatele duševního vlastnictví. Toto omezení se týká především zákonné bezúplatné licence, tzv. fair use (vysvětleno později). Z důvodu postavení crackingu mimo zákon bylo také možno postihovat osoby legitimní k prolamování hesel, především bezpečnostní odborníky a kryptology. Mezi další, ne příliš povedené, části zákona patří nemožnost vytvoření kopie díla pro vlastní potřebu nebo to, že každý z manželů musí mít svou vlastní licenci na autorské dílo apod.

- ***Virové hrozby***

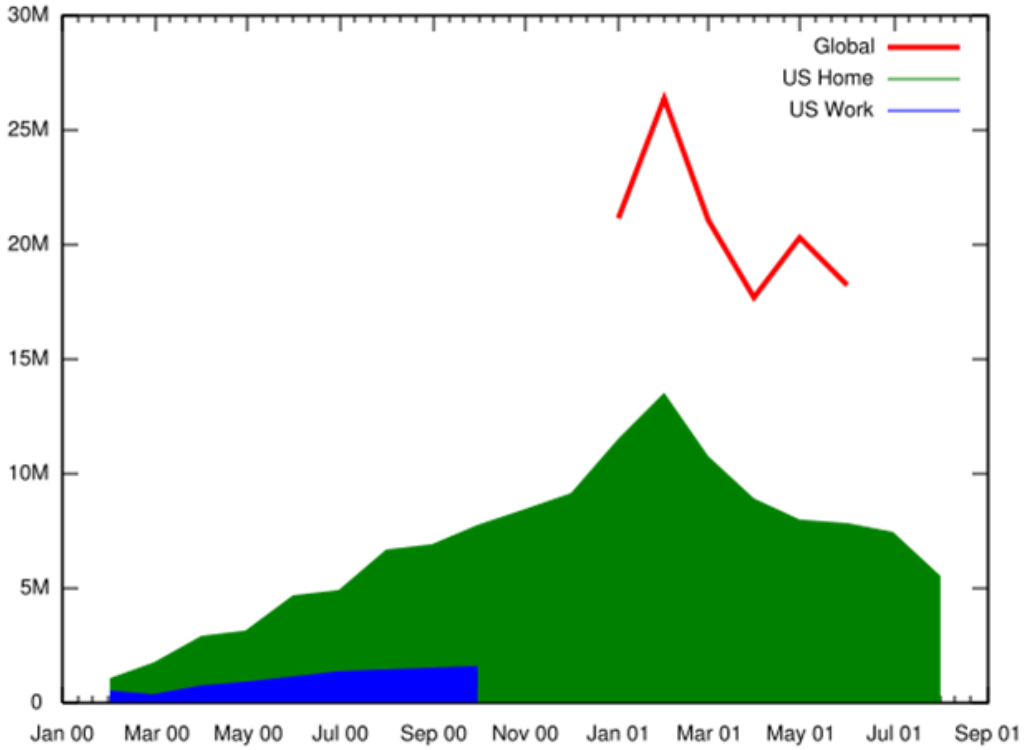
Mezi nejznámější viry „vypuštěné“ mezi lety 1999-2001 se stal vir „*Melissa*“ a „*I Love You*“. Funkce prvního z nich neměla destruktivní charakter. Systém šíření byl takový, že se tento vir rozeslal pomocí aplikace Outlook emailem na prvních padesát kontaktních adres z adresáře infikovaného počítače.

Druhý virus byl vytvořen v jazyce VBScript a pro jeho aktivaci byl nutný zásah uživatele v podobě spuštění souboru, který byl přiložený k emailu s předmětem ILOVEYOU. Do rozesílaných kopií byl přiložen spustitelný soubor, který mohl běžet na pozadí a vyhledávat čísla a hesla kreditních karet. Tyto údaje pak byly odeslány emailem zpět útočníkovi. Program také upravil systémové registry tak, aby se po každém zapnutí počítače sám spustil. Dále vir mazal některé systémové soubory nebo je měnil a obsah souborů se specifickými příponami (*.jpeg, *.vbs, *.css atd.) nahrazoval škodlivým kódem. U těch změněných souborů pak změnil koncovku na.vbs. Soubory s příponami.mp3 a mp2 byly nastaveny jako skryté. Navzdory tomu, že program, který mohl škodlivý kód z počítačů odstranit, byl veřejnosti uvolněn již 24hodin od propuknutí nákazy (5. května 2000), způsobil tento vir škody ve výši asi pět a půl miliardy dolarů. Zajímavostí je, že softwarový inženýr z Thajska, který napsal program proti tomuto viru, dostal o dva měsíce později nabídku místa konzultanta ve společnosti Sun Microsystems.

- ***Napster (1999-2001)***

Služba Napster byla síť typu P2P[5], která uživatelům umožňovala sdílet MP3 soubory. V provozu byla od června 1999 do července 2001. Svou funkcí obcházela klasické distribuční cesty hudebních souborů a tak byla zástupci hudebního průmyslu obviněna z hromadného porušování autorských práv. V dobách největšího rozmachu tuto síť používalo až několik desítek milionů lidí. Po vzoru této služby vzniklo mnoho dalších podobných programů, které umožňovaly a umožňují sdílení souborů systémem P2P, takže ačkoliv byla služba Napster soudním příkazem vypnuta, otevřela nový prostor službám podobného typu, které jsou díky svému počtu velmi těžko řešitelné. Značka a logo Napster byly odkoupeny a nadále provozovány jako placená služba.[6] Podle všeho by měla být služba stále v provozu, ale v době psaní diplomové práce jsou její stránky nedostupné z důvodu údržby.

Obrázek 1: Graf počtů uživatelů služby Napster v letech 2000 a 2001



Zdroj: Wikipedie: Otevřená encyklopedie. *Napster* [online]. 2. 9. 2010 [cit. 23.01.2011]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Napster.

[5] Peer-to-peer (doslova rovný s rovným), P2P nebo klient-klient je označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví klienti (uživatelé)

[6] Wikipedie: Otevřená encyklopedie. *Napster* [online]. 2. 9. 2010 [cit. 23.01.2011]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Napster>

- ***Nejznámější soudní procesy týkající se kyberprostoru ve světě***

V případu z roku 2000 byla americká firma Yahoo žalována u francouzského soudu francouzskou ligou proti rasismu (LICRA) za propagaci nacismu, protože přes aukční část portálu byly přístupné odkazy na nacistické materiály. Francouzský soud uznal Yahoo vinným. Když však chtěla americká pobočka ligy proti rasismu žalovat Yahoo v USA na výkon rozhodnutí, americký soud shledal, že rozhodnutí francouzského soudu užívalo restriktivnější právní úpravu, která byla s rozporem s Ústavou USA, konkrétně s prvním dodatkem zaručujícím svobodu projevu.

V roce 2001 byl po svém vystoupení na konferenci DefCon uvězněn Dmitrij Skljarov. Tento ruský kryptolog pracoval ve firmě ElcomSoft, která vyvíjela software na převod elektronických knih z chráněného formátu Adobe E-Book na nechráněný formát pdf. Ačkoliv byla tato činnost v Rusku zcela legální, státní zástupce argumentoval tím, že firma tento produkt nabízela na Internetu, mohli se k němu dostat i občané USA a tak byl spáchán jeho distribucí trestný čin. Proti žalobě se na celém světě zvedla vlna odporu v podobě výzev k bojkotu konferencí konaných v USA a firmy Adobe. Nakonec byla po půl roce obvinění proti Skljarovovi stažena a bylo mu uloženo, aby v celé kauze vystupoval jako svědek. Tento případ měl důležitý precedenční význam, neboť kdyby soud uznal postup amerických úřadů jako správný, činy v kyberprostoru by se přestaly posuzovat podle zákonů státu, ve kterém případné produkty vznikly, ale podle právních úprav států, ve kterých žijí uživatele, kteří by k produktu měli přístup. Dopad by byl v praxi takový, že subjekt nasazující softwarový projekt, by musel zkontrolovat právní úpravy všech států na světě. Pokud by tuto kontrolu neučinil, vystavoval by se nebezpečí, že bude v některém státě obžalován a při návštěvě zatčen.

- ***Situace na území ČR***

– CzERT byla hackerská skupina v prostředí českého a slovenského Internetu. V případě členů této skupiny šlo o hackery v původním smyslu slova, kteří brali hacking jako zábavu a proto nemohli být ani postihnuti, neboť podle právní úpravy by musel mít hacker ze své činnosti prospěch nebo způsobit škodu druhé straně. Navzdory neškodné činnosti provedla tato skupina mnoho povedených kousků a vtipů. Mezi nejznámější patří hack serveru ministerstva vnitra nebo úprava stránek serverů jako Seznam.cz, Mamedia nebo Mobilserver.

- Nejznámějším případem z oblasti porušování autorského práva byla kauza Minoret. Dne 22. listopadu 1999 bylo firmou Microsoft podáno trestní oznámení z porušování autorského zákona na společnost Minoret, s.r.o. zabývající se prodejem výpočetní techniky a černé elektroniky, kterou roku 1996 založil Miroslav Novotný. Trestní oznámení bylo podáno na základě kontrolního nákupu počítače špionem společnosti Microsoft u výše zmíněné firmy. Bylo zjištěno, že disk obsahuje software v hodnotě 17 000 Kč, ovšem při nákupu počítače nebylo za žádné programové vybavení zaplaceno. Policie ČR provedla razii, při která zabavila několik počítačů. O dva roky později však Ústavní soud ČR rozhodl, že policie použila při vyšetřování nezákonné postupy, a stíhání majitele společnosti bylo zastaveno.[7]
- V roce 2007, resp. 17. června, se povedlo umělecké skupině Ztohoven nabourat jednu z kamer, které vysílají v rámci pořadu Panorama a pustit předem připravený záznam atomového výbuchu v oblasti obce Černý důl v Krkonoších.

[7] Diit. *Kauza Minoret tajemství zbavená.* [online]. 29. 1. 2003 [cit. 15.02.2011]. Dostupný z WWW: <http://www.diit.cz/clanek/kauza-mironet-tajemstvi-zbavena/4541/>

2.2 Právní úprava počítačové kriminality

Dříve, než se začnu zabývat samotnou právní úpravou počítačové kriminality, uvedu charakteristiku základních pojmů, týkajících se diplomové práce.

Počítačová kriminalita

Pojem počítačová kriminalita se objevil v právní a kriminologické technologii vyspělých zemí již v sedmdesátých letech a masově v letech osmdesátých. V literatuře se můžeme setkat s více termíny označovanými jako počítačová kriminalita a to kybernetická kriminalita, kyberzločin, kriminalita informačních technologií nebo anglicky „IT crime" nebo „cybercrime". Oficiálních formulací počítačové kriminality existuje celá řada. Já si dovolím citovat některé z nich.

Počítačová kriminalita může být definována jako *„páchání trestného činu, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti nebo jako nástroj trestné činnosti".*[8]

Kybernetickou kriminalitu taky chápeme jako *„jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených".*[9]

Poslední vybraná definice je podle Prof. Ing. Vladimíra Smejkala, Csc.: *„Páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení včetně dat, případně některá z komponent počítače nebo většího množství počítačů samostatných, či propojených do počítačové sítě, a to buď jako předmět trestné činnosti nebo jako nástroj trestné činnosti."*[10]

Státy Evropské Unie a Evropského parlamentu se dohodly na následující definici počítačové kriminality: *„Je to nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím ICT nebo jejich změnu.".*[11]

---

[8] SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systému*. 1. vydání. Praha: C. H. Beck, 2001. 542 s. ISBN 80-7179-552-6. Str..480

[9] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 91

[10] SMEJKAL, V. *Internet a §§§*. 2. aktualit. a rozš. vyd. Praha: Grada Publishing, 2001. 284 s. ISBN 80-247-0058-1. Str. 151-152.

[11] Sborník z mezinárodní konference. *Bezpečnost v podmínkách organizací a institucí ČR*. [online]. 20. 5. 2005 [cit. 25.02.2011]. Dostupný z WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/sbornik.pdf>. Str. 31

Počítačová kriminalita se od klasické kriminality odlišuje specifickými charakteristikami (viz Příloha č. 4). Většinou se neobjevují prvky jako násilí, použití zbraně, ujma na zdraví apod. V klasické kriminalitě zákonodárci zjišťují dobu spáchání trestného činu na hodiny, minuty, kdežto trestný čin v oblasti počítačové kriminalitě může být spáchán bez přítomnosti pachatele na místě činu a v několika tisícinách sekundy. Charakteristickým rysem, který může také specifikovat počítačovou kriminalitu bývá diskrétnost trestné činnosti. Tato kriminalita je v literatuře označována jako kriminalita „bílých límečků".

Rozlišujeme velký počet kyberzločinů, kdy některé pouze využívají počítače pro páchání trestných činů a jiné se zaměřují na počítač. Více se o této problematice zmíním v kapitole č. 3.

Mezivládní organizace Rada Evropy, která sdružuje většinu evropských států, před pár lety vydala prohlášení o současných trendech, které nejsou vůbec povzbudivé. Bylo uvedeno, že:[12]

- dnešní informační společnosti jsou velmi závislé na informačních a telekomunikačních technologiích a stávají se tak, ve spojení s kybernetickým zločinem, značně zranitelnými
- viry, červi, trojští koně, škodlivé kódy se vyvíjí, šíří a využívají k různým podvodům, krádeži identity, praní špinavých peněz, apod.
- spamy představují většinu odeslaných e-mailů a začínají se objevovat i na mobilních telefonech jako lživé zprávy
- Internet se využívá pro sexuální zneužívání dětí a obchodování s lidmi

[12] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. 1. vydání Praha 2008. Auditorium. Str. 220. ISBN 978-80-903786-7-4. s.27 - 28

Počítačový útok

Počítačový (kybernetický) útok lze definovat jako operace za účelem přerušení, odepření, znehodnocení nebo zničení informací v počítačích či počítačových sítích nebo počítače či počítačové sítě samotné. Základem počítačového útoku je spolehnutí se na tok dat za účelem provedení útoku. Příkladem útoku může být použití počítačů za účelem způsobení úniku toxických chemikálií z výrobních a skladovacích prostorů, zhroucení elektráren, kolapsu rozvodných sítí.[13]

Tabulka 1 Srovnání bankovního přepadení a kybernetického útoku

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	pachatel riskuje, že bude zraněn či zabit	bez rizika fyzické újmy
Zisk	průměrně 3 – 5 tisíc USD	průměrně 50 – 500 tisíc USD
Pravděpodobnost dopadení	dopadeno 50 – 60 % útočníků	dopadeno cca 10 % útočníků
Pravděpodobnost odsouzení	odsouzeno 95 % dopadených útočníků	z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je odsouzeno jen 50 %
Trest	průměrně 5 – 6 let, pokud pachatel při loupeži nikoho nezranil	průměrně 2 – 4 roky

Zdroj: Cesnet. *Kybernetická kriminalita* [cit. 01.03.2011]. Dostupný z WWW: <http://www.cesnet.cz/akce/2009/bezpecnost-siti/p/kyberneticka-kriminalita.pdf>

Kyberterorismus

Mezi jednu z forem terorismu patří kyberterorismus, který je charakterizován jako vyšší stádium počítačové kriminality. Patří mezi největší nebezpečí 21. století, kdy pachatelům již nejde pouze o proniknutí na cizí internetové stránky, umístění obrázku a získání obdivu mezi hackery. Jejich cílem je především ovlivnění veřejného mínění či politických elit, resp. vyvolání strachu u široké veřejnosti.

„*Principem kybernetického terorismu je zneužívání výpočetní a telekomunikační techniky včetně Internetu jako prostředku a prostředí pro uskutečnění teroristického útoku*.“[14]

[13] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. 1. vydání Praha 2008. Auditorium. Str. 220. ISBN 978-80-903786-7-4, s. 51 -52

[14] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. ISBN 978-80-247-1561-2. Str. 288. Str. 129

Rozeznáváme dvě metody teroristických útoků:

1. Cílem útoku je zničení protivníkova informačního systému a systémů závislých na ICT (z anglického Information and Communication Technologies, označení informační a komunikační technologie)
2. Informační technologie jsou využívány jako nástroj útoku pro manipulaci a zneužití cizích informačních systémů, ke krádeži nebo změně dat, případně k přetížení a zahlcení informačních systémů

Softwarové pirátství

Softwarové pirátství je synonymem pro neoprávněné užívání softwaru, které je chráněného autorskými právy. K pirátství může dojít při kopírování, stahování, sdílení či prodeji softwaru. Další častou formou pirátství je instalace více kopií softwaru do osobního nebo pracovního počítače, než umožňuje zakoupená licence. Mnoho lidí si neuvědomuje, že při nákupu softwaru si nekupují vlastní software (program), ale jen licenci na jeho užívání. Tato licence určuje, jakým způsobem lze se softwarem nakládat. Například kolikrát lze software nainstalovat. Pokud je vytvořeno více kopií, než dovoluje licence, pachatel se dopouští pirátství.

Počítačové pirátství můžeme rozdělit do několika kategorií. Ty se mohou navzájem prolínat nebo si být alespoň velmi podobné. Ing. Vladimír Vacek rozlišuje:[15]

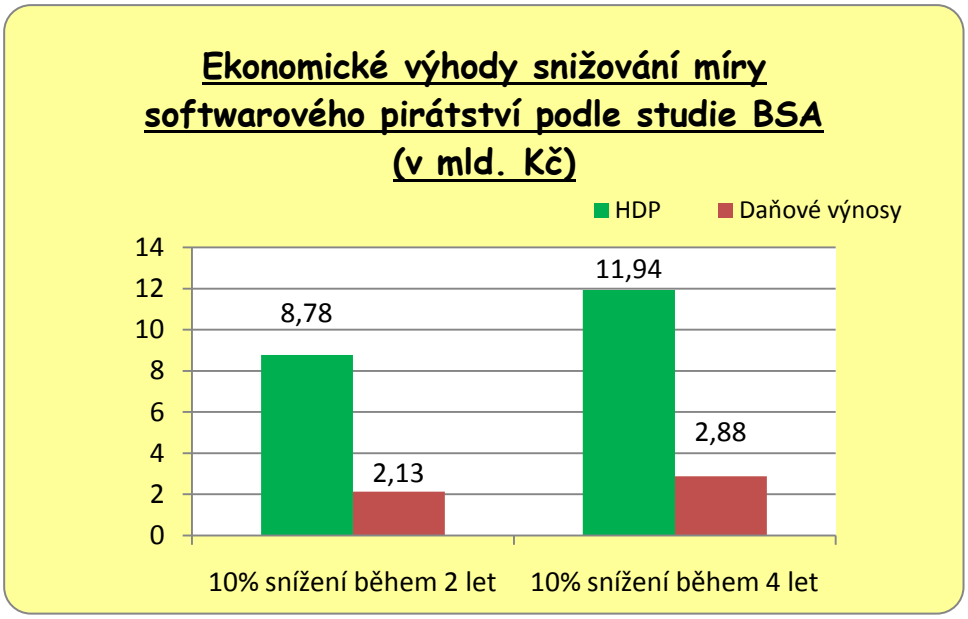
- *Pirátství koncových uživatelů* (End User Piracy) – charakteristické je používání obrovského počtu kopií daného softwaru na mnoha počítačích
- *Domácí pirátství* (Home Piracy) – zde patří činnosti jako vyměňování CD a DVD s přáteli a provozování nevýdělečné internetové stránky s cílem nelegálně distribuovat programy
- *Pirátství prodejců* (Reseller Piracy) – pirátství se dopouštějí samotní prodejci při prodeji počítačů s ilegálně nainstalovaným programem
- *Pirátství probíhající na Internetu* (Internet Piracy) – uživatelé Internetu stahují legální softwary a pak je kopírují bez licence
- *Pirátství podniků* (Corporate Piracy) – bez licence se k nelegálně nainstalovanému programu připojí v lokální společnosti několik set zaměstnanců
- *Průmyslové pirátství* (Industrial Piracy) – skupiny či jednotlivci, za účelem získání majetkového prospěchu, kopírují a distribuují programové vybavení

[15] Sborník z mezinárodní konference. *Bezpečnost v podmínkách organizací a institucí ČR.* [online]. 20. 5. 2005 [cit. 25.02.2011]. Dostupný z WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/sbornik.pdf>

Mezi nejčastější rizika související s používáním nelegálního softwaru patří riziko trestního postihu, riziko ztráty dat, riziko virové nákazy počítače, riziko finanční ztráty a riziko ztráty soukromí. Rizik je velká spousta a proto není od věci si licenci k softwaru dobře přečíst.[16]

Mezinárodní organizace Business Software Alliance (BSA), která po celém světě prosazuje práva softwarového odvětví, ve své nedávné[17] studii uvedla, že snižování tuzemské míry softwarového pirátství má pozitivní dominový efekt na celou ekonomiku. Konkrétně uveřejnila, že díky snížení softwarového pirátství o 10 procent by během příštích čtyř let mohlo dojít k vytvoření 1085 pracovních míst v technologickém odvětví, do ekonomiky by přiteklo 8,78 miliard korun a na daních by stát do roku 2013 vybral o 2,13 miliard korun více. V případě rychlejšího snížení softwarového pirátství, resp. místo čtyř let během dvou let, daňové výnosy by vzrostly až o 36 procent (viz Obrázek 2).

Obrázek 2: Ekonomické výhody snižování míry softwarového pirátství



Zdroj: Business Software Alliance. *Ekonomické výhody snižování softwarového pirátství podle studie BSA*. [online]. 15. 8. 2010 [cit. 21.02.2011]. Dostupný z WWW: <http://www.bsa.org/country/News%20and%20Events/News%20Archives/global/09152010-piracyimpact.aspx>

[16] Business Software Alliance. *Co je softwarové pirátství?* [online]. [cit. 21.02.2011]. Dostupný z WWW: <http://www.bsa.org/country.aspx>.
[17] 15. září 2010 v Praze

2.2.1 Charakteristika hlavních skutkových podstat

Česká republika si dosud vystačila v trestním zákoně č. 140/1961 Sb. s jedinou normou (§ 257a Poškození a zneužití záznamu na nosiči informací), která primárně chránila důvěru, integritu a dostupnost počítačových dat a systémů. Návrh na změnu tohoto zákona byl připravován patnáct let a k 1. lednu 2010 vešel v platnost nový trestní zákoník č. 40/2009 Sb., který obsahuje celou řadu novinek včetně změn postihů a úprav různých druhů počítačové kriminality.[18]

Objektem původní úpravy § 257a Poškození a zneužití záznamu na nosiči informací byla ochrana počítačových dat uložených na nosiči informací proti neoprávněným změnám, zničení nebo neoprávněnému použití a ochrana počítače před neoprávněnými zásahy. Postihována byla změna software a neoprávněné užití informací uložených na nosiči, resp. odcizení dat. Směšné na celé věci bylo to, že přirozeně nikdo vůbec nepochyboval o zaměření ustanovení na hardware, či přesněji řečeno na nosič informací. Přitom ovšem pojem „nosič informací“ nebyl nikde definován tak, aby vylučoval použití jiného než digitálního nosiče.[19]

Aby byla naplněná skutková podstata trestného činu poškození a zneužití záznamu na nosiči informací, bylo nezbytné pachatelem úmyslně[20] získat přístup k nosiči informací, získat takový přístup v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, informací z tohoto nosiče neoprávněně užít, nebo takové informace zničit, poškodit nebo učinit neupotřebitelnými, nebo učinit zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení.

Pro představu uvedu případy kdy byli, v souběhu s jinými trestnými činy, odsouzeni pro naplnění skutkové podstaty podle § 257a tito pachatelé:

- policista, který v policejních databázích vyhledával údaje o osobách,
- bývalý jednatel, který smazal účetnictví firmy poté, co byl odvolán,
- zaměstnanec televize, který zasahoval do počítačového programu pro losování loterie provozované televizí a umožnil vyhrávat spřízněným osobám,

[18] Právní rádce. *Postih počítačové kriminality podle nového trestního zákona.* [online]. 22. 7. 2009 [cit. 08.03.2011]. Dostupný z WWW: < http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

[19] Tamtéž

[20] *Trestný čin je spáchán úmyslně, jestliže pachatel a) chtěl způsobem v tomto zákoně uvedeným porušit nebo ohrozit zájem chráněný tímto zákonem, nebo b) věděl, že svým jednáním může takové porušení nebo ohrožení způsobit, a pro případ, že je způsobí, byl s tím srozuměn.*

- zaměstnanec banky, který s cílem vyprodukovat úroky z šesti termínovaných vkladů na neexistující společnost M., s. r. o., které nebyly kryty konkrétními vklady,

Nový trestní zákoník pojímá trestnou činnost počítačové kriminality jinak. Z původního ustanovení § 257a trestního zákona se stala dvě nová ustanovení, § 230 postihující neoprávněný přístup k počítačovému systému a nosiči informací a § 231 o opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Novým se stal i § 232 o poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. Přesné znění paragrafu je uvedeno v Příloze č. 2.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací [21]

Trestný čin podle § 230 v sobě zahrnuje pět různých jednání o počítačové kriminalitě, přesně neoprávněný přístup k počítačovému systému nebo jeho části, neoprávněný zásah do dat nebo do počítačového systému, falšování údajů souvisejících s počítači, podvod souvisejících s počítači a neoprávněný zásah do systému.

První odstavec normy upravuje postih neoprávněného získání přístupu k počítačovému systému[22] a zároveň postih překonání bezpečnostního opatření[23]. Jedná se o trestný čin úmyslný, kdy pachatel nemusí mít žádnou způsobilost a může jim být kdokoli. Jde o případ, kterému se říká „hacking“ (viz kapitola 3.1), kdy se pachatel zkouší nabourat do systému tak dlouho, dokud na heslo nepřijde.

Druhý odstavec upravuje postih dalšího možného jednání hackera či jiného osoby, která se již dostala do systému nebo získala přístup k nosiči informací[24]. Není ovšem důležité, jestli oprávnění k přístupu získala legálně či ilegálně. Základ je v tom, že osoba neoprávněně užije uložená data, neoprávněně vymaže uložená data nebo je jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu, případně je učiní neupotřebitelnými, padělá nebo pozmění uložená data tak, aby byla považována za pravá nebo neoprávněně vloží data do systému.

---

[21] ŠÁMAL, P. a kol. *Trestní zákoník II.* § 140 až 421. Komentář. 1 vydání. Praha: C. H. Beck, 2010, 2011 s. ISBN 978-80-7400-178-9.

[22] Počítačový systém je charakterizován jako zařízení sestávající se z technického (hardware) a programového (software) vybavení, které je určené ke zpracování dat.

[23] Bezpečnostní opatření je každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací.

[24] Nosičem informací je jakýkoli nosič dat, do kterého nebo na který lze zaznamenávat data a z kterého lze data zpět získat

Odstavec třetí normy upravuje úmysl způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch. Zákoník nevyžaduje žádnou nominální minimální výši a zároveň nemusí dojít k získání majetkového prospěchu, ale stačí, že pachatel jednal v tomto úmyslu.

Ustanovení odstavce čtvrtého postihuje jednání uvedené v odstavci prvním, pokud k němu došlo organizovanou skupinou, tedy sdružením více osob (dle soudní praxe sdružení nejméně tří trestně odpovědných osob) do něhož pachatel vstoupil a podílí se na jeho činnosti. Ustanovení čtvrtého odstavce postihuje též jednání, při kterém došlo ke značné škodě, čímž se rozumí škoda ve výši nejméně 500 000 Kč.

Pátý odstavec mluví o způsobení škody velkého rozsahu ve výši nejméně 5 000 000 Kč, tedy získání majetkového prospěchu pro sebe nebo pro jinou osobu.

§ 231 Opatření a přechovávaní přístupového zařízení a hesla k počítačového systému a jiných takových dat[25]

§ 231 je doplňkem k předchozímu § 230, kde objektem tohoto trestného činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nesrolovaného opatření a přechovávání zařízení, nástrojů a prostředků.

Norma vyžaduje úmysl spáchat trestný čin podle § 182 odst. 1 písm. b), c) nebo § 230 odst. 1,2 a jednání pachatele spočívající v opatření přístupového zařízení tím, že jej pachatel vyrobí, uvede do oběhu, doveze, vyveze, proveze nabídne, zprostředkuje, prodá nebo jinak zpřístupní sobě nebo jinému opatří.

Důvodem vzniku tohoto paragrafu je velké nebezpečí ohrožení zdraví a života osob při nedbalém nakládání s počítačovými systémy v mnoha odvětvích jako v obchodě, financích, letovém provozu nebo na jednotce intenzivní péče.

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti[26]

Objektem trestného činu podle § 232 je ochrana dat a technického či programového vybavení počítače před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda, tedy škoda dosahující částky nejméně 500 000 Kč. Pachatelem

[25] ŠÁMAL, P. a kol. *Trestní zákoník II.* § 140 až 421. Komentář. 1 vydání. Praha: C. H. Beck, 2010, 2011 s. ISBN 978-80-7400-178-9.
[26] Tamtéž.

může být jedna osoba, která vykonává zaměstnání, povolání, postavení nebo funkci, jednak i jiná osob, která porušila zákonem uloženou nebo smluvně převzatou povinnost.

Hlavní vybrané paragrafy, kterých se počítačová kriminality týká (přesné znění uvedených paragrafů konkretizuji v Příloze č. 3) jsou dále § 175 Vydírání, § 180 Neoprávněné nakládání s osobními údaji, § 182 Porušení tajemství dopravovaných zpráv, § 184 Pomluva, § 191 Šíření pornografie, § 206 Zpronevěra, § 207 Neoprávněné užívání cizí věci, § 209 Podvod, § 213 Provozování nepoctivých her a sázek, § 228 Poškození cizí věci, § 254 Zkreslování údajů o stavu hospodaření a jmění, § 268 Porušení práv k ochranné známce a jiným označením, § 269 Porušení chráněných průmyslových práv, § 270 Porušení autorského práva, práv souvis. s právem autorským a práv k databázi, § 317 Ohrožení utajované informace, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 357 Šíření poplašné zprávy.

V oblasti informatiky a telekomunikací jsou nejčastěji uplatňovány tyto základní zákony:[27]

- Obchodní zákoník neboli zákon č. 513/1991 Sb. Uplatňován bude v případech, kdy nelegální aktivity budou souviset se smluvním nebo podobným vztahem upraveným v tomto zákoně
- Občanský zákoník č. 40/1964 Sb. ve znění pozdějších úprav a jeho prováděcí předpis, kterým je nařízení vlády č. 258/1985 Sb. Důležitost tohoto předpisu je v tom, že jednoznačně definuje vlastnické právo a entity, proti kterým je kriminální činnost namířena
- Zákon o ochraně osobních údajů č. 101/2000 Sb. úzce související s ochranou telekomunikačního tajemství.
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů
- Zákon o elektronických komunikacích, pod číslem 127/2005 Sb. (původně telekomunikační zákon č. 151/2000 Sb.). Postihuje nezákonné chování subjektu v prostředí počítačové sítě, např. používání automatický systémů volání bez lidské

[27] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. ISBN 978-80-247-1561-2. Str. 288. Str.89 - 90

účasti pro účely přímého marketingu bez předchozího souhlasu dotčeného účastníka.

- Zákony související s ochranou průmyslového vlastnictví. Například zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví, dále zákon č. 441/2003 Sb., o ochranných známkách nebo zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti. Upravuje odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení. Společnost doufala, že zákon bude vhodným nástrojem boje proti spamu, avšak nestalo se.
- Zákon č. 40/1995 Sb., o regulaci reklamy
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 365/2000 Sb., o informačních systémech veřejné zprávy

Mezinárodní úprava počítačové kriminality

Možnost postihu trestných činů, jako je počítačová kriminalita a jevy souvisejících s prudkým rozvojem informačních technologií, narážejí na bariéry vyplývající z rozdílnosti právních řádů a na odlišnosti právních úprav v různých zemích.

Zásadním problémem je, že vnitrostátní právní normy mají vymezenou svoji působnost právě územím daného státu, kdežto v prostředí Internetu, který je globální a nezná hranice, ztrácí princip vymezení platnosti práva podle území smysl.

Pachatelé díky rozdílnosti právních úprav často využívají přesunu internetových aktivit, tedy jiné místo jednání pachatele a jiné místo účinků jednání, aby se vyhnuli trestní odpovědnosti, protože je pak složité určit rozhodné právo a příslušný soud.[28] Václav Jírovský z ústavu informatiky ČVUT tvrdí, že okrást nás může během stejné chvilky někdo z naší ulice i někdo z jiného světadílu. Konkrétně: „*Oběť byla z České republiky, pachatel komunikoval jakoby z Německa, ve skutečnosti ty informace šly přes Spojené státy, ale pachatel reálně komunikoval třeba z Itálie. Peníze ale šly do Rumunska. Stejně tak tomu bylo i opačně. Oběť byla v Německu, kanál byl velice podobný, ale peníze byly vybrané v České republice*“[29]

[28] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. 1. vydání Praha 2008. Auditorium. 220 s. ISBN 978-80-903786-7-4. Str.64

[29] Radiožurnál. Český rozhlas 1. *Představuje internet nebezpečí.* [online]. 27. 1. 2009 [cit. 01.03.2011]. Dostupný z WWW: <http://zpravy.rozhlas.cz/radiozurnal/podkuzi/_zprava/540206>.

Kyberkriminalita je navíc oblastí, u níž více než v případě jiných druhů kriminality platí, že právní úprava reaguje na jevy, které se nově objevují v reálném světě se zpožděním. To znamená, že takovéto protiprávní jednání neodpovídá žádné z existujících skutkových podstat, a tudíž nemůže být ani trestně stíháno.

Cestou vedoucí k možnému řešení tohoto problému je mezinárodní spolupráce a harmonizace internetového a počítačového práva cestou mezinárodněprávních nástrojů. Hlavním evropským a mezinárodním nástrojem k dosažení nastíněného cíle v oblasti počítačové kriminality je Úmluva Rady Evropy o počítačové kriminalitě (dále Úmluva).

Úmluva vznikla spolupráci expertů Rady Evropy, USA, Kanady, Japonska a dalších a byla schválena výborem ministrů Rady Evropy 8. listopadu 2001 v Budapešti. K Úmluvě by později připojen Dodatkový protokol o kriminalizaci některých činů s rasovým a xenofobním obsahem, který vstoupil v platnost 1. března 2005.

Ke dni 22. dubna 2008 Úmluvu podepsalo 44 států. Česká republika tuto Úmluvu podepsala v roce 2005, avšak dosud neratifikovala, stejně jako ji neratifikovala přibližně polovina (22 státu) dalších členů Rady Evropy.

Obsahuje společné definice různých druhů počítačové trestné činnosti a stanoví základy pro fungování soudní spolupráce mezi smluvními státy.

Velkým a zásadním problémem je i nadále existence rozdílu v samotné vnitrostátní úpravě. I po podpisu Úmluvy budou vedle sebe pořád existovat státy, které neratifikovaly žádný mezinárodní akt ohledně počítačové kriminality a tedy vycházejí s vlastní právní úpravy a státy, které jsou signatáři Úmluvy.[30]

[30] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. 1. vydání Praha 2008. Auditorium. 220 s. ISBN 978-80-903786-7-4. Str.103-105

3 Protiprávní jednání v prostředí počítačů a jejich pachatelé

V následující části diplomové práce se budu zabývat popisem protiprávního jednání v prostředí počítačů a jejich pachatelů. Na úvod vymezím pojmy jako právní norma, právní jednání a protiprávní jednání. Následně se budu zabývat rozdělením jednotlivých protiprávních jednání.

Právní norma

Pojem práva je neodmyslitelně spjat s termínem právní norma, který je základní stavební jednotkou právního řádu. Normu lze obecně chápat jako určité pravidlo vyjadřující „*to, co má být*". Stejná definice se dá použít i pro normu právní. Normy, podle Gerlocha, regulují chování lidí (přímo, nebo zprostředkovaně) a stanoví, jaké chování je z hlediska normotvůrce žádoucí a jaké nežádoucí.

Právní normu můžeme tedy definovat jako pravidlo chování, které je vyjádřeno zvláštní, státem uznanou formou (má podobu některého z pramenů práva), a jehož zachování je státní mocí vynutitelné.[31]

Rozdíl mezi určitým pravidlem chování a právní normou je v tom, že pravidlo musí splňovat určité znaky, aby se stalo právní normou. Znaky právních norem je možno rozdělit na formální a materiální.[32]

Mezi formální znaky patří původ právní normy a zákonem vymezené publikace. Materiální znaky jsou regulativnost, právní závaznost, obecnost a vynutitelnost státní mocí.

Právní a protiprávní jednání

Lidské chování je určitá schopnost, znalost a je výsledkem vědomí a vůle člověka. Způsob tohoto chování ve společnosti může velmi silně ovlivnit život každého z nás. Vzhledem k právní normě můžeme toto chování rozdělit na jednání právní a jednání protiprávní.

[31] Business center.cz. *Právní norma.* [online]. [cit. 13.02.2011]. Dostupný z WWW: <http://business.center.cz/business/pojmy/p707-pravni-norma.aspx>.
[32] KNAPP V., *Teorie práva*. Praha: C.H.Beck, 1995, s. 148

Právní jednání

Právní jednání nebo také právní úkon je dle občanského zákoníku definován jako projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojuje.

Právní jednání můžeme rozdělit na právní úkony a individuální právní akty. Právní úkony jsou jakýmsi druhem právní skutečnosti, spočívající v projevu vůle fyzické nebo právnické osoby, který směřuje ke vzniku, změně nebo zániku subjektivních práv a povinností. Individuální právní akty jsou také projevem vůle, ale v tomto případě orgánů veřejné moci, kterými rozhodují o právech a povinnostech.[33] Jde například o rozhodnutí správního orgánu o přidělení bytu, rozsudek o osvojení dítěte.

Protiprávní jednání

Protiprávní jednání lze také označit termínem delikt, který spočívá v projevu vůle, který je v rozporu s právními normami.[34] Existují lehčí a těžší případy porušení práva, které právní řád zná. Při lehčím porušení zákona dochází „pouze“ ke skutečnému nebo symbolickému vrácení do *statu ante quo* (stav jako před konfliktem) například kompenzací, odškodněním, bolestným či zadostiučiněním. V opačném případě, tedy při porušení právních norem, které vážně ohrožují právní řád, je již zakročeno rázněji. Taková protizákonná jednání bývají nazývána trestnými činy.[35]

Této části kapitoly budu věnovat větší pozornost a zaměřím se na popis jednotlivých forem počítačové kriminality. Počítačovou kriminalitu je možné rozdělit podle postavení počítače při páchání trestné činnosti na protiprávní jednání proti počítači, kdy počítač je terčem útoku a protiprávní jednání s počítačem, kdy počítač je nástrojem protiprávní činnosti.[36]

[33] GERLOCH, A. *Teorie práva*. 5. Vyd. Plzeň: Aleš Čeněk, 2009. 308 s. ISBN 978-80-7380-233-2. Str.145
[34] Tamtéž. Str.147
[35] HARVÁNEK, J. a kolektiv. *Teorie práva*. Plzeň: Aleš Čeněk, 2008. 501 s. ISBN 978-80-7380-104-5. Str. 306
[36] MATĚJKA, M. *Počítačová kriminalita*. Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 52

3.1 Protiprávní jednání proti počítačům

Protiprávní jednání proti počítačům můžeme definovat jako útok směřující proti počítači jako hmotnému předmětu, proti technickým prostředkům informačního procesu, tj. sběru, přenosu, uchování, zpracování a distribuci dat. Tento útok je uskutečňován prostřednictvím výpočetní techniky. Nyní uvedu jednotlivé typy útoku a jejich popis.[37]

Krádež

Trestný čin krádeže je upraven v § 205 Trestního zákon v hlavě páté a je obecně definován jako neoprávněné přisvojení si cizí věci. V případě, že dojde k odcizení počítače samého či dílů ještě nesestaveného počítače, je tento čin považován za trestný.[38]

Podle statistik Policie ČR bylo pouze za první čtvrtletí roku 2010 provedeno 2 297 krádeží za účelem odcizení počítačů. Dále statistika uvádí, že nejčastěji jsou počítače odcizeny, pokud je jejich majitel ponechá bez dohledu v autě. Krádež počítačů může znamenat ztrátu velice citlivých informací, a proto si myslím, že bychom tuto hrozbu neměli podceňovat.

Loupež

O trestný čin loupeže (§ 173 TZ) se bude jednat, když při přepadení bude lupičem odcizen notebook, či jiný podobný předmět. Za porušení tohoto trestného činu může být pachatel potrestán odnětím svobody na dvě léta až deset let.[39]

Zpronevěra

Zpronevěra je trestný čin upravený v § 206 TZ. Čin, jehož se dopustí ten, kdo si přisvojí cizí věc nebo jinou majetkovou hodnotu, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou (škoda dosahující částky nejméně 5 000 Kč).[40]

Průmyslová špionáž

Pod pojmem průmyslová špionáž je možno si představit průnik do systému konkurence a zneužití jejich dat a důvěrných informací. Příkladem mohou být utajené

[37] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení* [cit. 15.02.2011]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>.
[38] Zákon č. 40/2009 Sb., trestní zákoník
[39] Zákony online. [online]. [cit. 14.02.2011]. Dostupný z WWW: <http://zakony-online.cz/>.
[40] Business center.cz. *Zpronevěra.* [online]. [cit. 14.02.2011]. Dostupný z WWW: <http://business.center.cz/business/pojmy/p1193-zpronevera.aspx>.

obchodní informace – např. o strategických záměrech firmy nebo poptávce či nabídce na trhu s cennými papíry na kapitálovém trhu. Uvedený zločin existoval dávno předtím, než vznikl počítač, ovšem později právě počítačový fenomén páchání tohoto trestného činu zjednodušil. K provedení průmyslové špionáže bývá nejčastěji využíváno hackerského útoku nebo infikování hostitelského počítače virem.[41]

Společnosti po celém světě začínají průmyslové špionáži přikládat stále větší význam, nejen při samotné obraně, ale také v získávání nejnovějších informací o konkurenčních společnostech. Kvůli mediálně známé špionážní aféře ve francouzské automobilce Renault (tři nejvyšší manažeři společnosti byli obvinění z poskytování tajných informací třetím osobám) došlo v poslední době ke zvýšení zájmů veřejnosti o průmyslovou špionáž a krádeže dat.[42]

Hacking

Hacking je považován, vedle porušování autorských práv, za jednu z nejvýraznějších oblastí počítačové kriminality, která s sebou přináší bohatou historií, proto se budu touto problematikou zabývat podrobněji.

Termín „hacking“ vznikl zhruba v padesátých letech minulého. Díky událostem zmíněných v kapitole o historii počítačové kriminality, se dostal do podvědomí lidí. Opravdový rozvoj hackingu se začal projevovat až v osmdesátých letech, kdy vznikly první hackerské skupiny, které vzájemně spolupracovaly a vyměňovaly si přístupové kódy a zjištěná hesla z počítačů.

[41] MATĚJKA, M. *Počítačová kriminalita*. Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 52

[42] iHNed.cz. *Průmyslová špionáž: hlavní podezřelý je Čína. Jak se bránit?* [online]. 9. 2. 2011 [cit. 14.02.2011]. Dostupný z WWW: < http://ekonomika.ihned.cz/c1-49977460-prumyslova-spionaz-hlavni-podezrely-je-cina>

Tabulka 2 Přehled významných útoků na přelomu století

Rok	Událost
1988	Národní banka v Chicagu se stává obětí počítačového podvodu za 70 milionů dolarů
1995	Ruští hackeři převedli 10 milionů dolarů z Citibank na svá konta
1996	U. S. General Acounting Office zveřejnil zprávu, že došlo k 250 000 útoků na počítače ministerstva obrany, z toho 65 % bylo úspěšných
1999	Prezident Clinton podepsal nárůst výdajů o 1,46 miliardy dolarů na zvýšení bezpečnosti vládních počítačů
2000	Jsou ukradeny zdrojové kódy Windows a Microsoft Office
2002	Microsoft přerušuje vývoj systému Windows, osm tisíc programátorů je vyškoleno pro oblast bezpečnosti

Zdroj: Jirovský,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 49

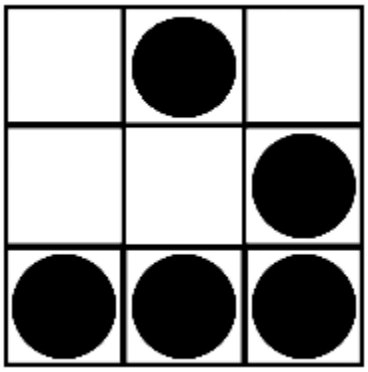
Hacking je anglický pojem, který lze definovat jako „*proniknutí do počítačového nebo řídícího systému jinou než standardní cestou při obejití nebo prolomení jeho bezpečností ochrany*“.[43] Co se týče právní úpravy, je průnik do systému trestný podle § 230 TZ, který hovoří o neoprávněném přístupu k počítačovému systému a nosiči informací.

Pachatel hackingu je označován termínem „hacker“. Hacker je člověk, který vyniká ve znalostech využívání hardwaru počítače nebo je expertem ve využívání konkrétního programu. Můžeme jej také definovat jako experta nebo nadšence v daném vědním oboru. Mnoho hackerů provádí tuto činnost jen pro zábavu a proniknutí do určitého systému berou jen jako dosažení touženého vítězství. Díky novinářské nevědomosti jsou tito hackeři v myslích prostých lidí prezentování jako kriminální individua, která ničí internetové stránky ve snaze získat choulostivé osobní údaje jiných uživatelů či narušit

[43] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 102

informační systém. Ovšem opak je pravdou. Hacker je intelektuální osoba, která má snahu dennodenně dokazovat svoji zručnost v oboru.[44]

OBRÁZEK 3 Hackerský emblém



Zdroj: Jirovský,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 50

Stejně jako v každé jiné společnosti i v hackerské komunitě existují různé typy osobností. Můžeme je rozdělit do následujících skupin:[45]

1. ***Script Kiddies*** (případně Wannabes) – jedná se o mladé hackery s průměrnými znalostmi programování a počítačů. Jsou schopni proniknout do systému dlouho známými bezpečnostními dírami. Po jejím proniknutí většinou data vymažou a nechají vzkaz: „Byl jsem tady. Fantomas.“.
2. ***White Hats*** – označování jako „hodní“ hackeři a prakticky nezpůsobují žádné škody. Jsou najímání firmami a na žádost majitele napadnou systém s cílem najít bezpečnostní slabiny.
3. ***Black Hats*** – uskutečňují podobnou činnost jako „White hats“, ale s cílem systém napadnout a získat pro sebe či někoho jiného výhody. Respektive účelem jejich činnosti je obohatit se, a tudíž jsou nazývání jako „crackeři".
4. ***Grey Hats*** – stojí na pomezí skupin „White hats“ a „Black Hats“. V případě, že se dostanou do počítače, data nesmažou ani nezneužijí, ale ani neopraví bezpečnostní díru, kterou v počítači našli.
5. ***Elite*** – hackeři, kteří se proslavili nejlegendárnějšími kousky.

[44] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 51
[45] MATĚJKA, M. *Počítačová kriminalita*. Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. s. 54

Aby mohli hackeři svou nekalou činnost provádět, potřebuji k tomu určité hackerské nástroje. Jirovský ve své publikaci Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství dělí tyto techniky do několika skupin:

- *hardwarové nástroje*, kde můžeme zařadit např. techniky hledání bezpečnostních děr v čipových kartách
- *softwarové (programové) nástroje*, které patří mezi nejčastější. Jsou to např. programy pro získávání hesel (keyloggery, bruteforce attack nástroje)
- *sociální inženýrství* je způsob získávání důležitých informací od uživatelů bez jejich vědomí, že toto činí

Nyní si dovolím uvést tři kategorie těchto nebezpečných programů (označovány souhrnně jako Malware):[46]

1. ***Viry***

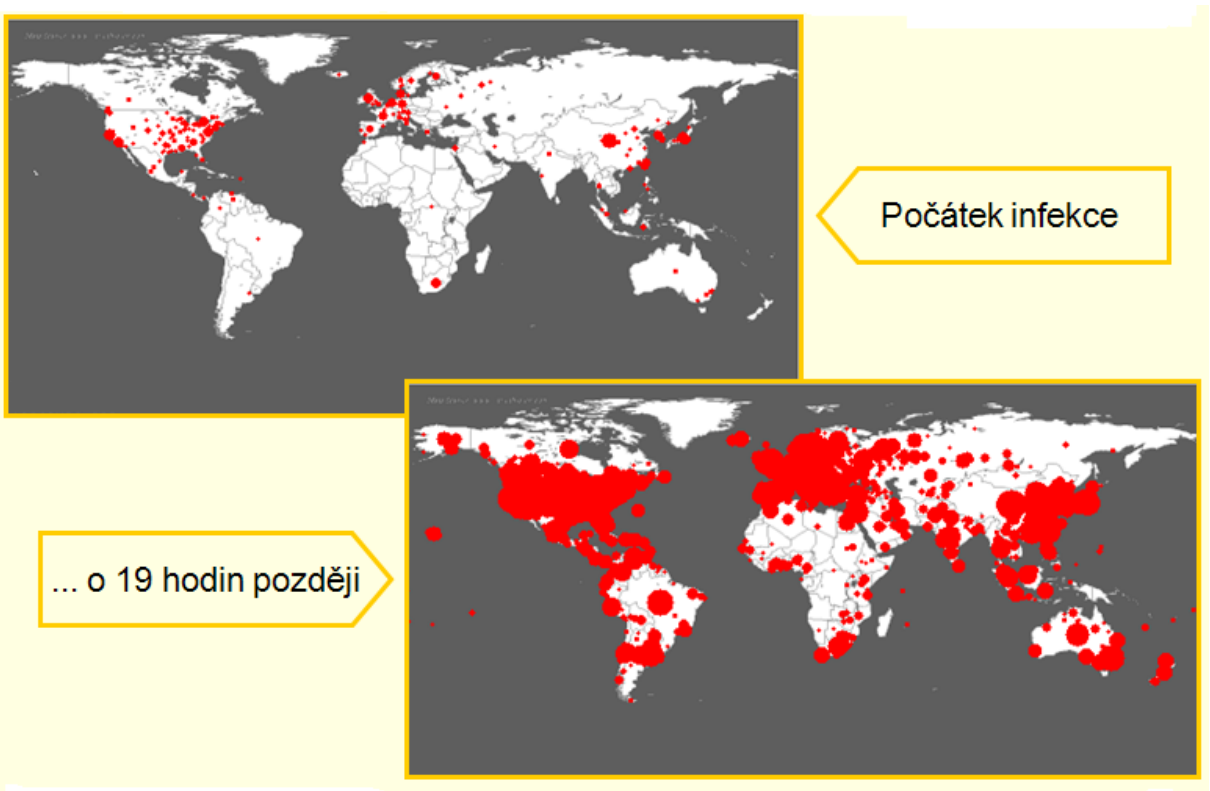
   Název je odvozen z podobnosti chování těchto programátorských produktů s biologickým originálem. Viry jsou programy, které se dokážou bez vědomí uživatele samy šířit. Virus připojí sám sebe k hostitelskému souboru a poté se pokusí šířit z počítače do počítače. Může i nemusí škodit. Šíří se jako humor či reklama nebo, v tom horším případě, maže či mění soubory. Odhaduje se, že každý asi 320. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.[47]

2. ***Červi***

   Červ má stejnou schopnost jako virus, automaticky kopírovat sám sebe, bez nutnosti připojení se k jinému souboru, či programu z jednoho počítače do jiného a šířit se mezi počítači pomocí informačních kanálů, sítí a e-mailů. Jakmile se ocitne v systému, je schopen rozesílat kopie všem členům e-mailového adresáře a může způsobit zpomalení celého procesu zobrazování webových stránek na Internetu. V následujícím obrázku je vidět rychlost šíření síťového červa Code Red.

[46] Microsoft. *Co je to virus, červ a trojský kůň?* [online]. 12. 5. 20008 [cit. 15.02.2011]. Dostupný z WWW: <http://www.microsoft.com/cze/athome/security/viruses/virus101.mspx#E2C>
[47] VOLEVECKÝ, P. *Kybernetické hrozby a jejich trestně právní kvalifikace.* Trestní právo č. 12/2010. s. 8. ISSN 1211-2860.

Obrázek 4 Rychlost šíření Malware - Code Red



Zdroj: Základní definice vztahující se k tématu kybernetické bezpečnosti. [cit. 25.02.2011]. Dostupný z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>

3. ***Trojští koně („trojan horses“)***

   Trojští koně ve smyslu počítačových programů fungují na podobném principu jako Trojský kůň z řecké mytologie. Jeví se jako programy z legitimního zdroje, avšak po spuštění mohou napáchat mnoho škod. Trojští koně se šíří díky důvěřivosti uživatelů v obsah většinou neznámých emailů. Někteří trojští koně byli součástí upravených aktualizací zabezpečení produktů firmy Microsoft.

Carding a phishing

Mezi další dva druhy protiprávního jednání s využitím počítače patří carding a phishing.

Vznik **cardingu** souvisí s rozvojem internetového obchodu a je chápán jako zneužití platebních karet. Ke zneužití platební karty může dojít několika způsoby. K nejprimitivnějším způsobům patří krádež čísla platební karty nebo krádež karty samotné.

Dříve bylo možné využít programy (tzv. generátory), pomocí kterých bylo vygenerováno číslo kreditní karty a zneužito. Od té doby však platební systém prošel zdokonalovacím procesem, kdy se při použití platební karty ověřuje nejen její číslo, ale i online autentizace uživatele např. zasláním SMS na mobilní telefon vlastníka účtu. Proto již dnes není použití tohoto systému možné.

Carding je jedním z mála typů počítačové kriminality, kde je více rozšířená činnost organizovaných skupin a to hlavně ve fázi získávání platebních karet a provádění možných triků.

Mezi nejstarší a nejoblíbenější patří tzv. libanonská smyčka. Při ní se do otvoru pro vložení karty v bankomatu umístí smyčka z magnetofonového pásku. Ta při vložení kartu zachytí a zabrání jejímu vyjmutí. Majitel karty je přesvědčen, že karta byla v bankomatu zadržena, a odchází přesvědčen o nutnosti návštěvy pobočky banky (o vyžádání vrácení karty). Po jeho odchodu ale podvodníci kartu z bankomatu pomocí smyčky bez problémů vytáhnou a v nejkratším možném čase okopírují. Protože však ubývá karet pouze s klasickým magnetickým „proužkem" a přibývá karet čipových, je nutné zjistit také pin. K tomuto účelu může sloužit miniaturní kamera, která nahraje vaše zadávání pinu na klávesnici bankomatu.[48]

Tuto oblast protiprávního jednání upravuje § 249b zákona č. 140/1961 Sb., trestního zákona, neoprávněné držení platební karty. *„Kdo si neoprávněně opatří nepřenosnou platební kartu jiného, identifikovatelnou podle jména nebo čísla, nebo předmět způsobilý plnit její funkci, bude potrestán odnětím svobody až na dvě léta, nebo peněžitým trestem nebo propadnutím věci."*[49] Dále je oblast upravena dle okolností konkrétního činu § 209 TZ, podvod, § 230, neoprávněný přístup k počítačovému systému a nosiči informací či § 180, neoprávněné nakládání s osobními údaji.[50]

Druhým internetovým podvodem je **phishing**. Podvodníci se snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svoje obohacení. Pro příklad uvádím v Příloze č. 1 názornou ukázku phishingového podvodu.[51]

K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky a snaží se přesvědčit uživatele, aby

[48] KRATOCHVÍL, P. *Nejnovější triky internetových zlodějů.* CHIP elektronický časopis o počítačích a digitální technice. 2010, č. 4 [online]. [cit. 15.02.2011]. Dostupný z WWW: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2010/chip-06-2010/nej-triky.>.
[49] Zákon č. 40/2009 Sb., trestní zákon
[50] MATĚJKA, M. *Počítačová kriminalita*.Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 57-59
[51] Hoax. *Phishing.* [online]. 3. 1. 2011 [cit. 14.02.2011]. Dostupný z WWW: <http://www.hoax.cz/phishing/internetove-bankovnictvi-rb-20110104/>.

kliknul na odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde jsou po něm požadovány přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně vyplní, získají tato data podvodníci, kteří je následně využijí pro svůj prospěch.

3.2 Protiprávní jednání s využitím počítačů

Protiprávní jednání s využitím počítačů je druhou kategorií reprezentující protiprávní jednání s využitím informačních technologií. Počítače při nich slouží výhradně jako nástroj trestné činnosti. Za pomoci počítačů dochází velmi často například k porušování autorského zákona (nedovolené kopírování a zneužívání softwarových produktů, hudebních nosičů aj.).

I další trestné činy dostaly s rozvojem technologií novou podobu. Počítače znamenají velké usnadnění v mnoha situacích.

Padělání a pozměňování peněz

Trestného činu padělání a pozměňování peněz se dopustí ten, kdo padělá nebo pozmění peníze v úmyslu udat je jako pravé nebo platné anebo jako peníze vyšší hodnoty, nebo kdo padělané nebo pozměněné peníze udá jako pravé a ten, kdo sobě nebo jinému opatří padělané nebo pozměněné peníze, nebo kdo takové peníze přechovává, bude potrestán odnětím svobody na dvě léta až osm let.[52]

V dřívějších dobách bylo padělání peněz nebo také veřejných listin úkolem pro ty nejšikovnější kreslíře a rytce, ovšem v dnešní době je to činnost padělatelských gangů. Jejich členové umí ovládat příslušný software, používají ty nejdokonalejší tiskárny, skenery, barevné kopírky, resp. investují do kvalitní technologie tisku. Právě díky těmto druhům podvodů je stále více kladen maximální nárok na ochranné prvky peněz, cenin a jiných dokumentů či dokladů.[53]

V roce 2009 bylo zadrženo 3 684 padělaných a pozměněných českých bankovek a mincí, kdy nejčastějším padělkem byla tisícikoruna, z mincí pak dvoukoruny a pětikoruny. Vrchní ředitel ČNB Pavel Řežábek řekl, že i když počet padělků vzrostl, nebyly

[52] Zákon č. 40/2009 Sb., trestní zákon
[53] MATĚJKA, M. *Počítačová kriminalita*.Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 62

zaznamenány větší problémy vůči české měně. Ve větším měřítku jsou samozřejmě padělány měny, které jsou používány na rozsáhlejším území. Tisková zpráva Evropské centrální banky uvádí, že v prvním pololetí 2010 bylo zadrženo 387 000 euro bankovek.

Letadla

Jedna z typických vlastností člověka je touha po rychlém popř. bezpracném zisku. Cest k dosažení tohoto cíle je velké množství. Patří zde například finanční hry typu letadel či pyramid. V minulosti byly hry typu Letadlo hrány na papíře, ale s rozmachem IT technologií se přesunuly do prostředí počítačů a Internetu. Masivní rozšíření těchto her vedlo zákonodárce k novele trestního zákona vložením ustanovení o provozování nepoctivých her a sázek (§ 213 TZ).[54]

Podstatou her je přerozdělování finančních prostředků vložených hráči do hry. Účastníci, nacházející se na vrcholu pyramidy, získávají peníze na úkor účastníku na nižších místech. Jedním ze způsobů, jakým je hra nabízená, je formou e-mailů, které upozorňují na snadnost výdělku této báječné letadlové investice.

Další cestou k dosažení bezpracného zisku jsou, podle Matějky, i jiné podvody jako je vylákání peněz za neexistující služby či falešné e-shopy. Tyto e-shopy ovšem nejsou na Internetu evidovány ve velkém množství. Podle výkonného ředitele Asociace pro elektronickou komerci je větší pravděpodobnost okradení kapsářem v tramvaji, než okradení při nákupu na Internetu.

Šíření pornografie

Trestný čin šíření pornografie upravuje § 191 trestního zákona v hlavě III. Trestnímu stíhání se vystavuje kdokoliv, kdo vyrábí, dováží, vyváží nebo distribuuje pornografické dílo, v němž se projevuje násilí nebo neúcta k člověku či je zobrazen pohlavní styk se zvířetem. Pachateli může být udělen zákaz činnosti nebo propadnutí věci či může být poslán do vězení až na jeden rok.[55]

Dále může být postihnuta osoba, která pornografické dílo zpřístupňuje dětem nebo je zveřejňuje na místech přístupných dětem. Tomuto pachateli hrozí trest ve výši odnětí svobody až na dvě léta, zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty.

---

[54] SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systému*. 1. vydání. Praha: C. H. Beck, 2001. 542 s. ISBN 80-7179-552-6. Str. 504

[55] Bezplatná právní poradna. [cit. 15. 02. 2011]. Dostupný z WWW: <http://www.bezplatnapravniporadna.cz/online-zdarma/ruzne/skutkove-podstaty-trestnych-cinu/3266-trestny-cin-sireni-pornografie-191-trestniho-zakoniku-hlava-iii-trestne-ciny-proti-lidske-dustojnosti-v-sexualni-oblasti.html>

V minulosti se pornografie prodávala z ruky do ruky v tmavých ulicích především pomocí obskurních časopisů. Dnes patří pornografický průmysl k nejdynamičtěji se rozvíjejícím odvětvím. Podle různých odhadů je jeho roční obrat 4,9 až 60 miliard amerických dolarů, z čehož mají zhruba 55% podíl Spojené státy americké.[56]

Na Internetu je k dispozici ve velkém množství, a tak pro dnešního uživatele počítače s připojením k Internetu není problém pornografické materiály stahovat, sdílet a prohlížet.

Hoax

Tento typ trestné činnosti je velmi nebezpečný v tom, že dokáže skutečně ovlivnit chování mnoha uživatelů Internetu. Spočívá v šíření nepravdivých či poplašných zpráv (hoaxů), šíření více či méně uvěřitelných historek a vyvolávání paniky prostřednictvím Internetu. Zprávy či historky mají tzv. osud běžce v tom smyslu, že obíhají světem v obrovském počtu řetězových emailů. „*Charakteristické pro ně je, že obsahují především emotivní sdělení, tváří se jako akt mezilidské solidarity, která živí jejich přenos, jejich smyšlený charakter není často na první pohled zřejmý*.“[57]

Jako příklad uvedu pár druhů varovných emailů, s kterými se určitě každý z nás již setkal: *Chcete-li mi zachránit život, pošlete tento mail na adresu American Cancer Society. Za každý mail mi tato organizace přispěje na léčbu nevyléčitelné osteoporézy jater částkou… Chcete-li vyjádřit svoji solidaritu afgánským ženám, pošlete tento mail co největšímu počtu Vašich známých a forwardujte jej na adresu…Otevřete-li mail s názvem JOIN THE CREW, nahraje se do Vašeho počítače nový virus a smaže celý harddisk…*

Posledním uvedeným příkladem je varování o počítačových virech (virus hoaxe), které patří mezi nejčastější typy trestné činnosti. Zpráva je napsaná tak, aby vyvolala u příjemce pocit hodnověrnosti, a informuje o novém, fatálním a neodhalitelném viru.[58]

Spam

Pojem spam můžeme chápat v užším a širším slova smyslu. V užším slova smyslu mluvíme o spamu jako o hromadném šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu. Přesný podíl spamu v rámci emailové komunikaci nelze určit,

---

[56] Wikipedie: Otevřená encyklopedie. *Pornografie* [online]. 25. 1. 2011 [cit. 17.02.2011]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Pornografie>.

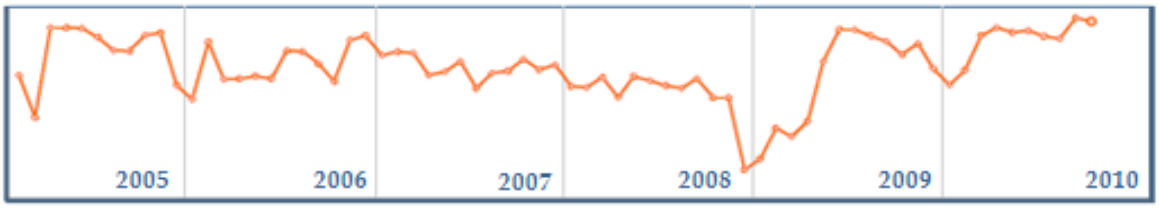
[57] ČINČERA, J. *Mha přede mnou, mha za mnou - hoaxes útočí na lidskou solidaritu*. Ikaros elektronický časopis o informační společnosti. 2002, roč. 6, č. 4 [online]. [cit. 15.02.2011]. Dostupný z WWW: <http://www.ikaros.cz/node/931>. ISSN 1212-5075.

[58] MATĚJKA, M. *Počítačová kriminalita*.Vydání první. Computer Press 2002. 108 s. ISBN 80-7226-419-2. Str. 68

ale např. společnost Symantec uvedla, že v říjnu roku 2009 spam představoval zhruba 88 % procent všech emailových zpráv a v září roku 2010 už činil spam 92,2 % ze všech emailových zpráv. Podle provedené analýzy společnost Symantec, kterou uveřejnila v lednu letošního roku, došlo k enormnímu poklesu množství nevyžádané pošty a spam nyní představuje pouze 78,6 % (1 ze 1,3 % e-mailů) všech e-mailů. Hlavním důvodem je, dle hlavního analytika společnosti Symantec[59], konsolidace a restrukturalizace gangů zaměřených na rozesílání farmaceutického spamu.[60] V širším slova smyslu mluvíme o spamu jako o všech doručených nevyžádaných zprávách. Předpokládá se neustálý nárůst spamu v elektronické komunikaci, ovšem Česká republika může být jako region klidná, protože pouze minimum (šest webů z tisíce) končících zkratkou .cz obsahuje škodlivé programy.[61]

Problematika spamu je řešena zákonem č. 480/2004 Sb., o některých službách informačních společnosti a o změně některých zákonů, který byl již třikrát novelizován. Poslední novelizace byla učiněna v roce 2007. Zákon ovšem nepracuje s pojmem spam, ale upravuje podmínky pro zasílání a přenos obchodních sdělení. Na dodržování tohoto zákona dohlíží Úřad pro ochranu osobních údajů. V případě, že má nevyžádaná pošta reklamní charakter a vede k nákladům na straně adresáta, může být tento čin ve správním řízení potrestán peněžitou pokutou až do výše dvou milionů Kč.[62]

OBRÁZEK 5 Vývoj nevyžádané pošty podle jednotlivých měsíců



Zdroj: Lupa.cz. *Nebezpečné emaily* [cit. 15. 02. 2011]. Dostupný z WWW: <http://www.lupa.cz/clanky/nebezpecne-emaily/>

Obtěžování emaily

V tomto případě se jedná ať již o obtěžování reklamními emaily, což se příliš za zločin považovat nedá, tak především obtěžující emaily se sexuálním a jiným obsahem.

[59] Paul Wood, MessageLabs Intelligence Senior Analyst, Symantec.cloud
[60] iHNed.cz. *Symantec: Množství spamu stouplo v říjnu na 88 procent* [cit. 09. 03. 2011] Dostupný z WWW: <http://digiweb.ihned.cz/c1-38973200-symantec-mnozstvi-spamu-stouplo-v-rijnu-na-88-procent> a <http://digiweb.ihned.cz/c1-37394600-emailove-schranky-zaplavuje-spam-jeho-podil-vzrostl-na-90-procent>
[61] VOLEVECKÝ, P. *Kybernetické hrozby a jejich trestně právní kvalifikace.* Trestní právo č. 12/2010. s. 6. ISSN 1211-2860
[62] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 104

Útočníci používají většinou SMS zprávy a emaily k tomu, aby osobám, kterým jsou zprávy určeny, znepříjemňovali život a útočili na jejich psychiku. Pachatelé přistupují k tomuto způsobu obtěžování obvykle pod záštitou anonymity na Internetu. V dnešní době je však možno pachatele velmi rychle vystopovat na základě kroků, které učiní. Pokud tuto činnost vyvíjí v podstatě amatér v oboru informačních technologií, pak je jeho dopadení více než pravděpodobné. Do skupiny lidí, kteří páchají tyto trestné činy, patří velmi často bývalí partneři obětí, známí nebo spolupracovníci.[63]

Kyber-stalking

Tento typ kyberzločinu je velmi podobný předchozímu případu. V tomto případě se však vyloženě jedná o psychické týrání, nebezpečné pronásledování oběti, kterou bývá obvykle bývalý partner[64]. Kyber-stalking je v podstatě stejný jako klasická forma stalkingu (způsob chování, kdy se pachatel zaměří na nějakého člověka, po němž potom slídí, pronásleduje ho, obtěžuje, hrozí mu, případně ho fyzicky napadá a ve vzácných případech dokonce usmrtí), liší se pouze prostředky, kterými k němu dochází. Cíle chování kyber-stalkera můžeme opět rozdělit do několika skupin.

Prvním typem je falešné obvinění, které útočník zveřejní a zpřístupní pomocí blogů, veřejných diskuzí apod., aby tak poškodil dobrou pověst své oběti. Stalkeři si mohou vytvořit své vlastní webové stránky věnované osočování a napadání osoby, na kterou útočí.

Dalším typem může být chování za účelem získání velkého množství informací o objektu svého zájmu a činí tak obvykle za nechtěné pomoci spolupracovníků, přátel nebo rodinných příslušníků své oběti nebo dokonce využívá služeb soukromého detektiva. Pokud je útočník zdatnější v používání informačních technologií, často se pokouší získat IP adresu počítače oběti, aby mohl přímo sledovat provoz na jejím počítači.

Často se stalker uchýlí k tomu, že do obtěžování a napadání své oběti nějakým způsobem donutí některé další osoby z řad přátel nebo rodiny. Poskytne třetí straně telefonní a emailový kontakt, aby také mohla útočit na osobu, kterou si zvolil za cíl svého zájmu.

---

[63] Zlínský deník. *Obtěžování přes internet řeší policie a počítačoví experti.* [online]. 7. 2. 2011 [cit. 06.03.2011]. Dostupný z WWW: <http://zlinsky.denik.cz/zpravy_region/obtezovani-pres-internet-resi-policie-a-pocitacovi.html>.

[64] Wikipedie: Otevřená encyklopedie. *Cyberstalking* [online]. 28. 2. 2011 [cit. 06.03.2011]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cyberstalking>.

Mezi vážné typy chování patří to, kdy útočník křivě obviní svou oběť, že ona obtěžuje jeho nebo je schopen aktivně a vědomě ničit věci, které jsou ve vlastnictví oběti. V souvislosti s kyberprostorem se jedná především o vytváření a zasílání virů nebo jiných škodlivých kódů za účelem poničit počítač a jiná elektronická zařízení nebo o získání soukromých informací oběti.

Útočník často objednává jménem oběti různé služby a zboží přes Internet. Obvykle se jedná o časopisy se sexuální a erotickou tématikou nebo erotické hračky a jako místo doručení uvádí adresu podniku nebo budovy, kde je pronásledovaná osoba zaměstnaná.

V neposlední řadě se stalkeři pokoušejí o navázání kontaktu nebo zorganizování setkání s obětí a to mnohdy pod záštitou cizí, neznámé identity nebo naprosto anonymně.

Warez

Warez, který je výsledkem nástupu moderních informačních technologií a výsledkem rozmachu Internetu, lze popsat jako moderní počítačové pirátství. Warez můžeme také chápat jako obsah se kterým je zacházeno nelegálně, tedy v rozporu s autorským zákonem.

Historie warezu je delší než historie Internetu. Nelegální kopírování hudby na počátku umožňovaly již audio kazety, či pirátské šíření filmů na videokazetách. S nástupem nových nepřepisovatelných technologií CD-ROM a DVD, kdy se zdálo, že se Warez vytratí, se objevily vypalovací zařízení, které činily a činí pirátské kopie levnější, než originál.[65]

Slovo bylo vytvořeno z anglického slova *wares* (*zboží*, zřejmě v souvislosti se slovem softwares). Nejčastějším způsobem šíření warezu je dnes hlavně Internet a šíří se často s odstraněnými ochranami proti kopírování.[66] Šíří se jak pomocí P2P sítí, které umožňují výměnu hudebních souborů, videí a dalších, tak i po nechráněných FTP serverech (server pro nahrávání a stahování souborů pomocí protokolu FTP) a sdílením souborů na serverech služeb typu RapidShare, Ulozto, Hellshare atd.

Tuto oblast trestného činu lze kvalifikovat jako porušení autorských práv, na kterou se vztahuje § 270 trestního zákona, který umožňuje uložit peněžitý trest nebo trest odnětí svobody až na dva roky (za jistý okolností zvýšena až na pět let).

---

[65] JIROVSKÝ,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 68

[66] Wikipedie: Otevřená encyklopedie. *Peer to peer* [online]. 11. 2. 2011 [cit. 15.02.2011]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Peer-to-peer>.

3.3 Pachatelé

Trestní zákon rozeznává tři formy pachatelství: samostatné pachatelství, nepřímý pachatel a spolupachatel.[67]

Pachatel trestného činu je podle zákona ten, kdo trestný čin spáchal sám, nikoliv společně s jiným pachatelem.

Nepřímým pachatelem je ten, kdo úmyslně užije ke spáchání trestného činu jinou osobu jako „živý nástroj“. Přičemž „živý nástroj“ odpovědný není nebo jen omezeně.

Typickým znakem nepřímého pachatelství je úmysl nepřímého pachatele spáchat trestný čin prostřednictvím jiného. V praxi se může jednat o případy zneužití osoby nepříčetné nebo dítěte.

Spolupachatelství spočívá ve spáchání trestného činu společným jednáním (objektivní podmínka) a zároveň musí spolupachatel mít úmysl ke společnému jednání (subjektivní podmínka). Při odpovědnosti spolupachatelů zákon stanoví, že pokud byl trestný čin spáchán společným jednáním dvou nebo více osob, odpovídá každý z nich, jako by trestný čin spáchal sám.

Uvedený druhy pachatelství jsem popsala obecně ve smyslu trestního zákona. Nyní se zaměřím na samotné pachatele počítačové kriminality.

Pachatelé počítačové kriminality

Pachateli trestných činů v oblasti kybernetické kriminality jsou v převážné většině případů kvalifikované osoby, tedy osoby se středoškolským nebo vysokoškolským vzděláním v oboru informačních technologií. Tito pachatelé bývají nadprůměrně intelektuálně vybavení a kreativní a zásadně jednají individuálně. Stávají se jimi, protože ve svém pracovním zařazení nejsou ocenění a spokojení. Motivem pachatelů může být získání pocitu beztrestnosti nebo neodhalitelnosti, kompenzace pocitu křivdy, odstranění pocitu vykořisťování zaměstnavatelem a touha po riziku nebo dobrodružství. Převažujícím motivem, který pachatele vede k počítačové kriminalitě, je touha po zisku.

Pachatele počítačové kriminality můžeme, z hlediska vztahů těchto pachatelů k informacím, dělit na amatéry a na profesionály.

[67] JELÍNEK, J. a kolektiv. Obecná část . *Trestní právo hmotné*. 1. vydání, Praha 2004. Linde Praha, a.s. 470 s. ISBN 80-7201-501-X. Str. 278

Amatéři jsou osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa. Mezi amatéry bychom mohli zařadit hackery, neúspěšné kritiky, mstitele a crackery. Hackeři, nebo také „průnikáři“ pronikají do systému s cílem prokázat své schopnosti a kvality (viz kapitola 3.1). Další skupinou mohou být neúspěšní kritici, kteří většinou opakovaně poukazují na závady či nedostatky v informačních systémech a nutnost jejich řešení. Do skupiny amatérů dále patří mstitelé, které, pro ně z nespravedlivých důvodů, propustil zaměstnavatel a oni mají, jak již ze samotného názvu vyplývá, tendenci se mstít. Crackeři patří také mezi amatéry, jejichž cílem je nabourávání se do informačního systému a získávání dat. Ovšem nemají zájem data ve svůj prospěch využít. Uspokojení nastává spíše z porušení systému.

Za **profesionály** jsou v tomto případě považování novináři, podnikatelé či zaměstnanci tajných služeb, jejichž náplní v zaměstnání je informační proces, tj. získávání, shromažďování, analyzování a využívání informací. Do této kategorie můžeme zařadit i softwarové piráty, jejichž cílem je neoprávněný zisk z prodeje nelegálně získaného softwaru.[68]

[68] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení* [cit. 15.02.2011]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>.

4 Příčiny a důsledky počítačové kriminality

4.1 Příčiny počítačové kriminality

Jedním z hlavním důvodů vzniku informační kriminality byl průnik do systému ve snaze odstranit chyby a pro jeho využití jej optimalizovat. Tento důvod byl činěn čistě s legitimním oprávněním. Avšak z historickým vývojem IT a s masovým využitím počítačů se kriminalita stala opravdovou. Průniky do systému měly destruktivní charakter a pro pachatelé bylo zajímavější ukradení dat z počítače či elektronická loupež na bankovním účtu.

Michal Matějka ve své publikaci uvádí několik faktorů, které jsou obecně příčinou počítačové kriminality a případně ji usnadňují:

1. ***Složitost informačních technologií a jejich provozu***

Můžeme bez obavy říci, že rychlost vývoje informačních technologií je obrovská. Nevyvíjí se jen technologie, které se již používají, ale zavádějí se i technologie nové. Patří mezi ně nové programovací jazyky a nástroje, nové typy databází, serverů, síťových prostředků a jiných hardwarových součástí. S rostoucím tempem vývoje je více než kdy předtím důležitá schopnost IT odborníků přizpůsobit se novým a modernizovaným technologiím. Co se však stane, pokud se zločinec naučí nově nasazenou technologii používat lépe a rychleji než její provozovatel či administrátor?

Z logiky věci je jasné, že právě zde vznikají velké bezpečnostní mezery, kdy při jejich využití hackerem nebo jiným druhem počítačového zločince musí spojit síly mnohdy i víc počítačových odborníků, aby hrozbu eliminovali, zabránili jejímu šíření a v nejlepším případě pomohli útočníka nebo narušitele dopadnout.

Dalším úskalím nových technologií je jejich vzrůstající úroveň složitosti, protože čím více jsou systémy nebo zařízení složitější, tím hůře se v nich hledají chyby, kterých může případný útočník využít. Proto se dnes musí investovat velké prostředky do testování a kontroly výsledných produktů tak, aby byly možné nechtěné bezpečnostní chyby odstraněny a aplikace nebo technologie se staly pro uživatele bezpečnými.

2. *Důvěra uživatele ve výstupy z informačních technologií*

Lidé jsou dnes zvyklí používat počítač a Internet v podstatě celý den. Podle posledních výzkumů[69] je například návštěva Facebooku pro jeho uživatele první věcí, kterou ráno udělají. Jiní si při snídani pustí notebook a pročítají zprávy nebo použijí, v dnešní době velmi moderní, tablet k tomu, aby zjistili, co se za poslední dobu stalo. Z toho můžeme vyčíst velkou míru pozornosti, kterou uživatelé věnují zprávám v prostředí počítačů a internetu. Mnohdy se jedná o zkreslené bulvární zprávy, které svými palčivými titulky upoutávají pozornost. Lidé jsou k těmto zprávám, a nejen k nim, až nebezpečně důvěřiví a tento přístup se jim nemusí vyplatit. Uživatelé mají často pocit, že na internetu jim nic nehrozí, opak je však pravdou. Pokud například útočník nějakým způsobem zkreslí nebo dokonce zveřejní svou vlastní zprávu s poplašným obsahem na některém informačním serveru s velkým počtem návštěvníků, hrozí, pokud si čtenář informaci neověří, hromadná panika. Pokud se zpráva týká některého odvětví, týkajícího se společnosti, s jejímiž akciemi obchodují burzovní makléři, pak hrozí poklesy indexů i prudké výkyvy v cenách akcií, které mohou vyústit až v nestabilitu regionálních ekonomik.

3. *Objem dat v prostředí, kde se pachatelé pohybují*

Objem dat na internetu se podle statistik každý rok asi zdvojnásobí. Podle údajů z konce roku 2010 se jedná o asi 500 milionu TB dat[70], které se v prostředí internetu nacházejí (viz. Příloha č. 5). Na obrázku vytvořeného podle údajů z konce října 2010 můžeme vidět několik zajímavých věcí. Mezi zajímavosti určitě patří to, že vyhledávač Google má pro vyhledávání zaindexovaných „pouze“ 200 TB dat, což je asi 0,0004 % z celkového objemu dat. Pokud si ale uvědomíme, že obyčejná webová stránka má velikost v průměru asi 500 kB, potom musíme konstatovat, že se jedná o obrovské množství stránek, které Google zpracovává. Další velmi rozšířenou službou s velkým obsahem dat je video server youtube.com, na kterém je každý den shlédnuto asi 2 biliony videí, dalších 24 hodin videí je nahráno každou minutu a nejoblíbenější videa mají počet zhlédnutí přes 60 000 každý týden. Z tohoto pohledu můžeme konstatovat, že objem dat na internetu je skutečně enormní a většina těchto dat může skrývat hrozbu, která může uživatele poškodit.

---

[69] Smseo. *42 % of People Check Facebook First Thing in Morning.* [online]. 8. 9. 2010 [cit. 14.03.2011]. Dostupný z WWW: <http://socialmediaseo.net/2010/03/25/check-facebook-in-mornging/>.

[70] Theroxor. *The Awesome size of the internet infographic.* [online]. 28. 10. 2010 [cit. 15.03.2011]. Dostupný z WWW: <http://theroxor.com/2010/10/28/the-awesome-size-of-the-internet-infographic/>.

4. Páchání trestné činnosti od obrazovky je snazší než v reálném životě

Snaha o „zjednodušení“ avšak také zrychlení dnešního života lidí je neoddiskutovatelná. A tak jako se mění způsob života, tak se mění i způsob konání zločinů, získávání informací, apod. Člověk s dostatečnými znalostmi a vybavením je dnes od počítače schopen prakticky čehokoliv, od špehování přes krádeže až po zabíjení lidí. Kterýkoliv zločin provedený od obrazovky počítače, je proveden pro pachatele bezpečněji, pohodlněji a je zde nepoměrně menší šance, že pachatel bude dopaden a ještě menší, že bude odsouzen, neboť shromažďování důkazů proti počítačovým kriminalníkům je stále velmi složitý úkon.

5. Nízké právní vědomí populace

Pokud lidé neví, že mohou být za něco postihnuti, popř. to ví, ale neví jakým způsobem, pak jim nemůže vadit, že jejich chování je nelegální, protože morální stránka např. používání nelegálního softwaru, je velmi složitá. Ještě složitější jsou normy, podle kterých by se lidé měli řídit. Velký počet lidí má v pojmech vyjadřujících moderní technologie značné mezery, tím méně mohou tušit, jak jsou tyto pojmy v zákonech upraveny.

6. Nedokonalost legislativy

Legislativa popisující počítačovou kriminalitu je ze samotné podstaty počítačové kriminality málo vyhovující. Nejenže je postavena na legislativě staré, která s podobnými skutky nemá vůbec nic společného, ale také se díky nepružnosti celého systému rozvíjí oproti zločinnosti v kyberprostoru, velmi pomalu. Nemůžeme se tedy divit, že lidé porušující autorské zákony a provádějící i další činy, mnohokrát uniknou spravedlnosti právě kvůli mezerám v zákoně.

V následujícím výzkumu, který jsem v rámci diplomové práce provedla, se pokusím objasnit faktory, které ze strany uživatelů PC přispívají k rozvoji počítačové kriminality.

4.2 Výzkum zaměřený na návyky, zkušenosti a názory uživatelů počítače

Cíl výzkumu

Cílem výzkumu diplomové práce byla analýza zaměřená na návyky, zkušenosti a názory uživatelů počítače. Jaké mají respondenti schopnosti a dovednosti s používáním PC, zda používají legální software a jestli si uvědomují, že jsou denně ohrožování počítačovými/internetovými hrozbami, co považují za největší hrozbu, či jak se brání proti těmto potenciálním napadením resp. jaký program k ochraně používají. Cílem bylo také zjistit, zda respondenti využívají sociální sítě a v čem podle nich existuje jejich největší nebezpečí.

Průběh výzkumu

V prvé řadě jsem si sestavila dotazník s otázkami (viz Příloha č. 7), abych mohla získat potřebná data. Informace a data můžeme rozdělit do dvou hlavních kategorií. Na data primární a data sekundární. V průběhu mého výzkumu jsem využila pouze data primárního charakteru, která byla zjišťována metodou dotazování, konkrétně formou elektronického dotazníku.

Abych předešla možnému neporozumění respondentů, provedla jsem pilotáž, kdy deset dobrovolníků vyplnilo dotazníky a následnou konzultací byly odstraněny nedostatky a chyby. Dotazník obsahoval 16 otázek, z nichž 2 byly identifikační a týkaly se věku a pohlaví respondenta.

Dotazování probíhalo v měsíci lednu 2011, kdy respondenti anonymně vyplňovali elektronický dotazník. Celkem jsem obdržela 182 vyplněných dotazníků a získaná data jsem zapsala do tzv. datové matice v programu Microsoft Excel verze 2007, kde jsem provedla vyhodnocení.

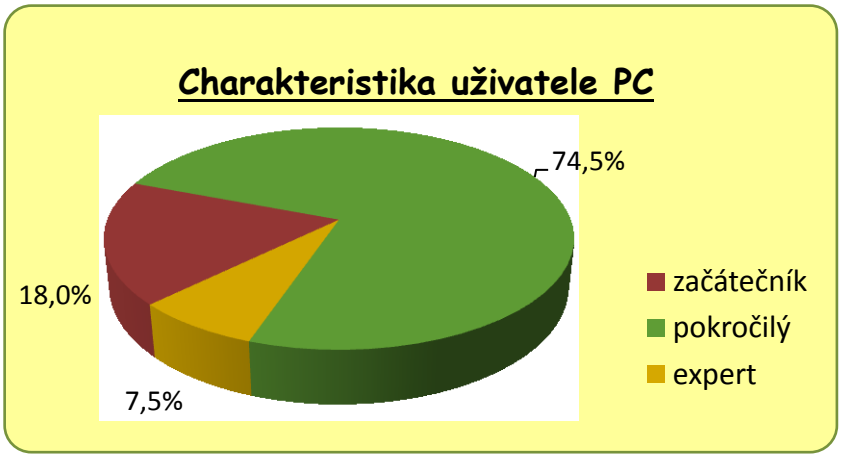
Analýza výsledků

Po získání potřebných údajů jsem pomocí programu MS Excel vytvořila grafy a tabulky, které mi nastínily některé další příčiny počítačové kriminality. Grafy, u kterých je součet hodnot větší než 100 %, znázorňují otázky, u kterých mohl respondent označit více než jednu možnost.

Vyhodnocení jednotlivých otázek

1. otázka: ***„Jak byste charakterizoval/a svoji schopnost/dovednost s ovládáním a využíváním počítače v životě?“***

Graf 1 Charakteristika uživatele PC

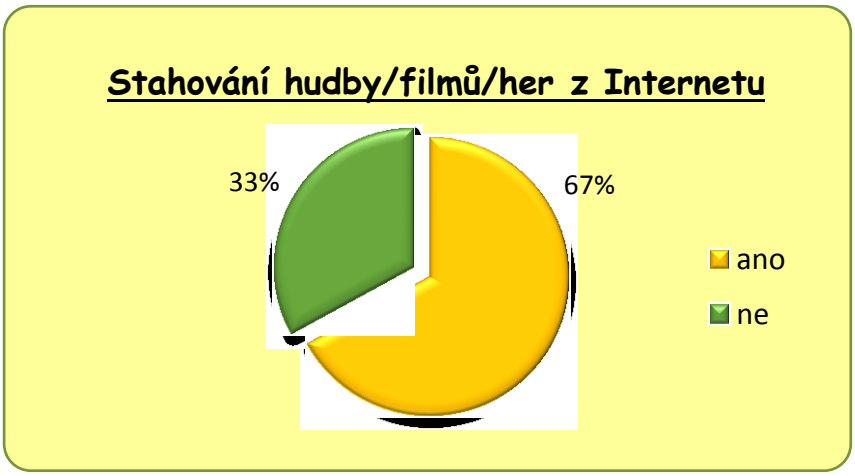


Zdroj: autorka

Většina dotazovaných (74,5 %) zhodnotila své schopnosti a dovednosti s využíváním počítače jako pokročilé. Jako začátečník by se označilo 18 % lidí a 7,5 % respondentů se považuje za experty.

2. otázka: ***„Stahujete z Internetu hudbu/filmy/hry?“***

Graf 2 Stahování hudby/filmů/her z Internetu

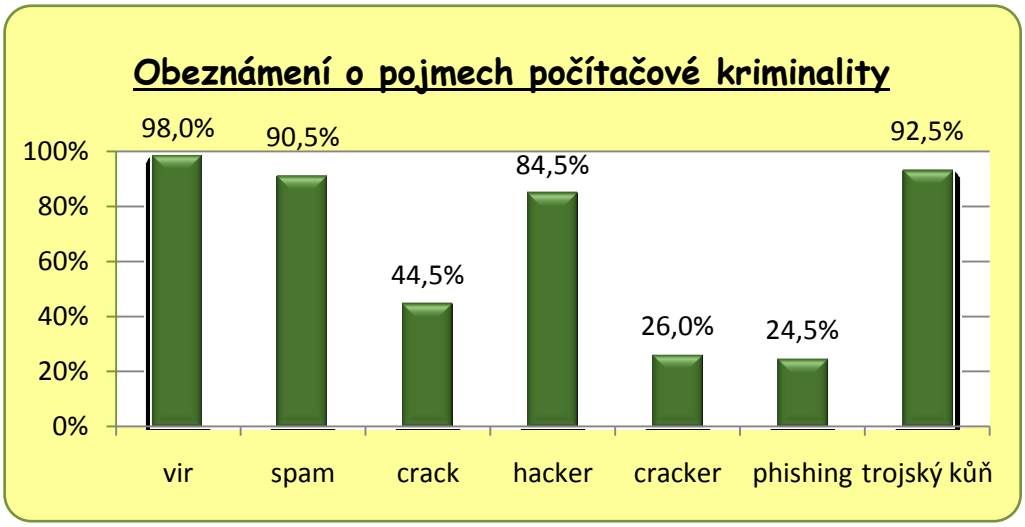


Zdroj: autorka

Z Internetu stahuje soubory podléhající autorským právům 67 % dotázaných. Zbývajících 33 % tyto typy dat nestahuje.

3. otázka: ***„Označte pojmy, o kterých může říct, že víte, co znamenají.“***

Graf 3 Obeznámení o pojmech počítačové kriminality

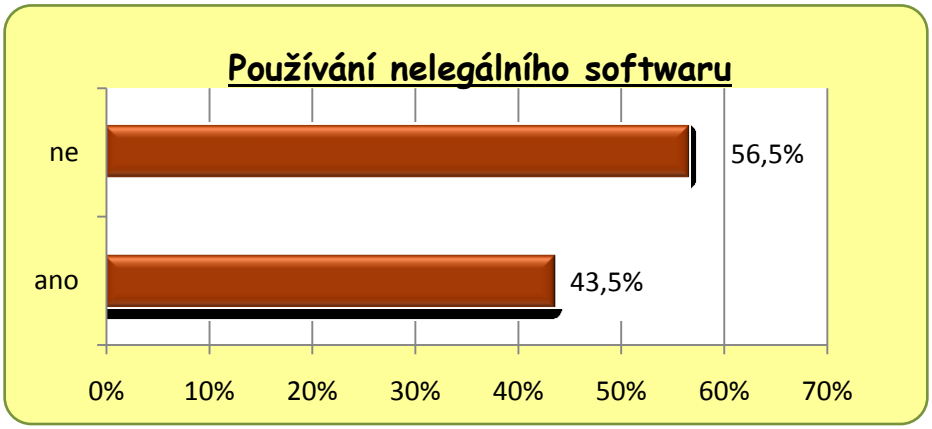


Zdroj: autorka

Z grafu vyplývá, že pojmy, týkající se kyber kriminality jsou mezi uživateli známé. Je otázkou, zda si pojmy vykládají opravdu správně. Nejlépe respondenti znali pojmy vir (98,5 %), trojský kůň (92,5 %), spam (90,5 %) a hacker (84,5 %). Další pojmy již dotazovaní znali méně. Pojem crack znalo 44,5 %, cracker 26 % a phishing 24,5 %. Dá se předpokládat, že vysoká znalost čtyř nejznámějších pojmů je způsobena jejich silnou medializací, kdy jsou významy některých slov často i zaměňovány.

4. otázka: ***„Používáte ve svém počítači nelegální software?“***

Graf 4 Používání nelegálního softwaru

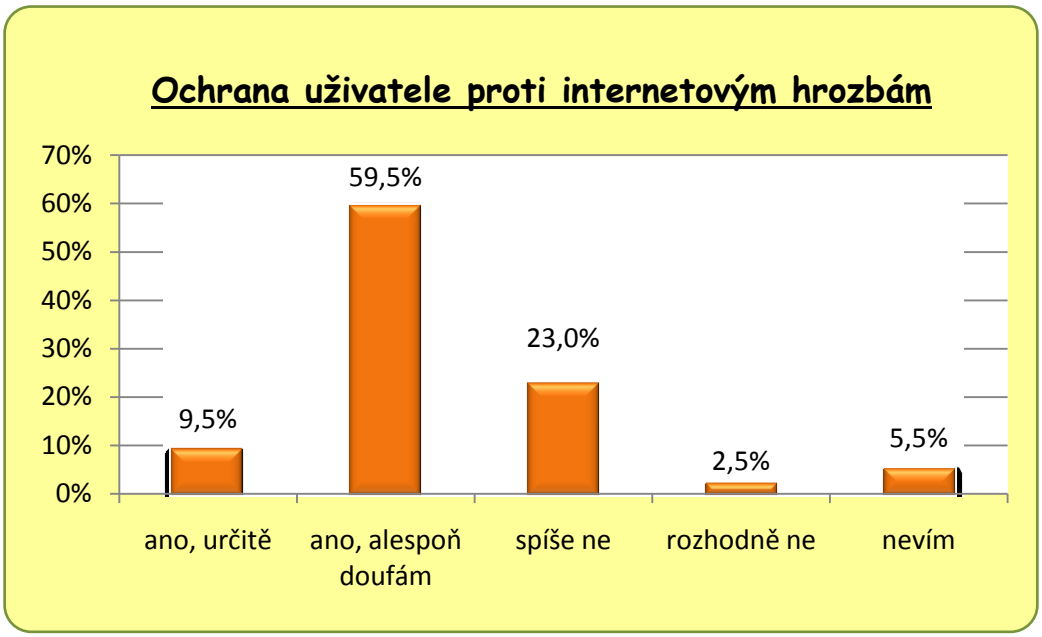


Zdroj: autorka

Různý nelegální software používá ve svém počítači 43,5 % respondentů. Zbývajících 56,5 % dotazovaných používá pouze legální licencovaný software nebo software nepodléhající licenci.

5. otázka: ***„Myslíte si, že jste dostatečně chráněni proti internetovým hrozbám?“***

Graf 5 Ochrana uživatele proti internetovým hrozbám

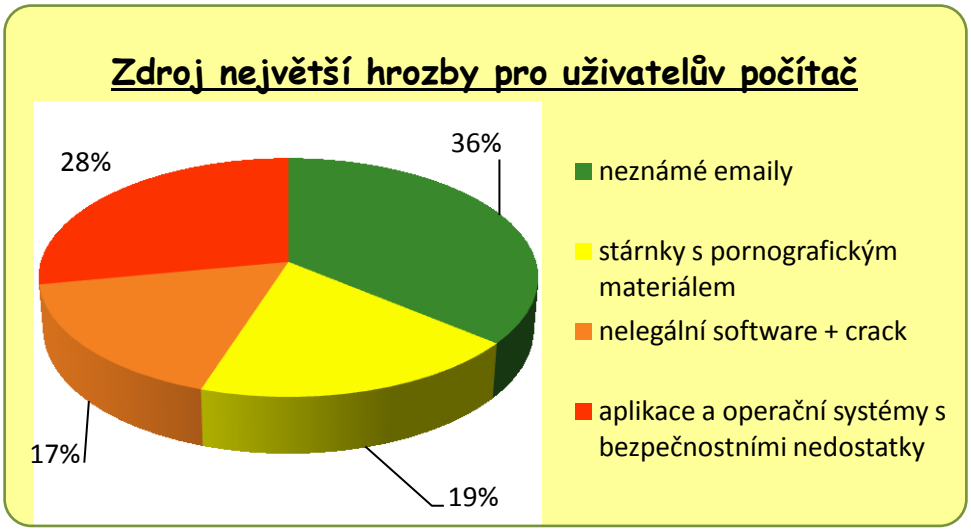


Zdroj: autorka

Z grafu vidíme, že si je pouze 9,5 % lidí, kteří vyplnili dotazník, naprosto jisto, že jsou dostatečně chráněni proti internetovým hrozbám. 59,5 % nemůže jistě říct, že jsou perfektně zabezpečeni, ale doufají v to. 23 % lidí si myslí, že dostatečně chráněni spíš nejsou, 2,5 % ví, že nejsou chráněni a 5,5 % neví. Jasně se zde ukazuje, že lidé stále nechápou nebezpečí hrozeb, které přicházejí z kyberprostoru.

6. otázka: ***„Jaký zdroj považujete za největší hrozbu pro Váš počítač?“***

Graf 6 Zdroj největší hrozby pro uživatelův počítač

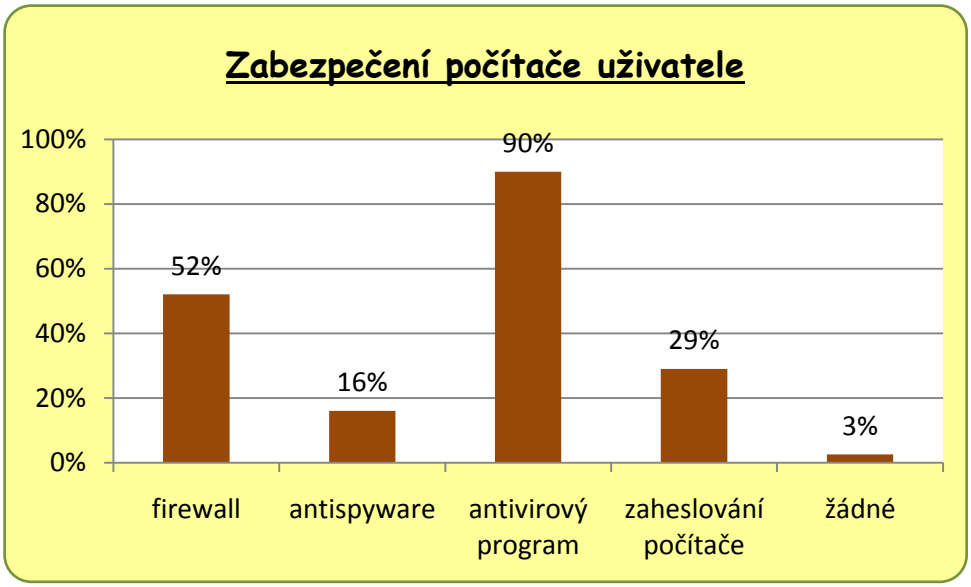


Zdroj: autorka

Tématem další otázky bylo to, co respondenti považují za největší hrozbu pro svůj počítač. Z neznámých emailů má největší strach 36 % lidí, 28 % se obává nedokonalostí dodávaných aplikací. Dalších 19 % dotazovaných má strach z ohrožení svého počítače obsahem stránek s pornografickými materiály. 17 % má pak strach z narušení prostřednictvím nelegálního softwaru.

7. otázka: ***„Které z následujících zabezpečení používáte?“***

Graf 7 Zabezpečení počítače uživatele

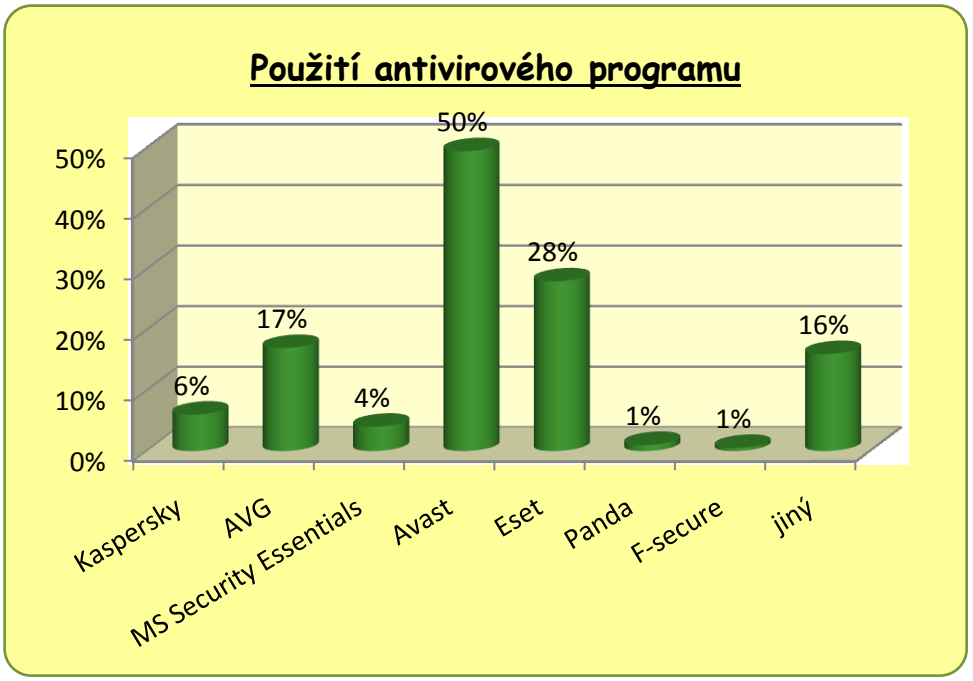


Zdroj: autorka

Průzkumem bylo zjištěno, že 90 % respondentů používá antivirový program. Firewall používá 52 % lidí. Menší zastoupení má používání zaheslování počítače (29 %) a antispywaru (16 %). Žádné z uvedených typů zabezpečení nepoužívají 3 % dotazovaných.

8. otázka: ***„Jaký antivirový program používáte?“***

Graf 8 Použití antivirového programu

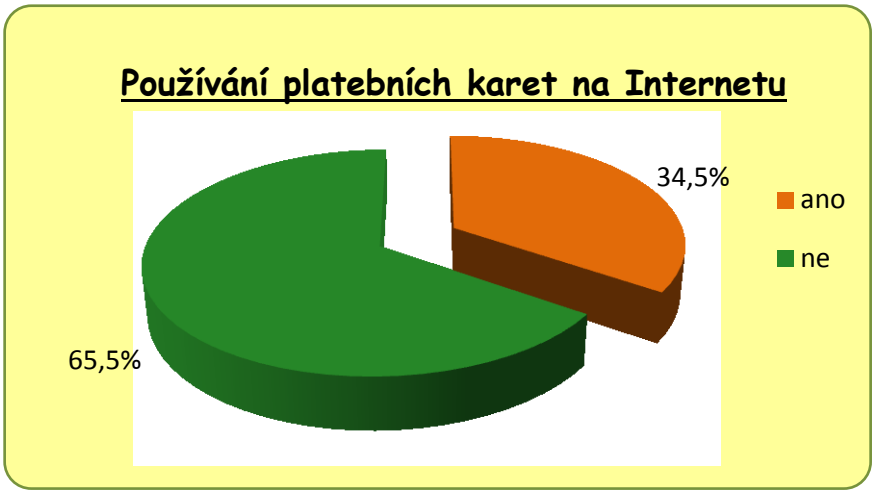


Zdroj: autorka

Z 90 % lidí, kteří ve svém počítači používají antivirový program, si zvolilo aplikaci Avast 50 % respondentů. 28 % používá produkt firmy Eset, 17 % preferuje program AVG. Menší díly v procentu užívání obsadily produkty Kaspersky (6 %), MS Security Essentials (4 %), Panda (1 %) a F-secure (1 %). 16 % dotazovaných používá jiný produkt.

9. otázka: ***„Platíte platebními kartami přes Internet?“***

Graf 9 Používání platebních karet na Internetu



Zdroj: autorka

Platebními kartami přes internet platí 65,5 % dotazovaných. Zbývajících 34,5 % karty pro internetové platby nepoužívá.

10. otázka: ***„Používáte internetové bankovnictví?“***

Graf 10 Používání internetového bankovnictví

Zdroj: autorka

Množství kladných odpovědí na používání internetového bankovnictví jsou téměř shodné s používáním platebních karet k platbám na internetu. Konkrétně odpovědělo kladně 70 % lidí a 30 % odpovědělo záporně.

11. otázka: ***„Máte strach ze zneužití Vašeho bankovního účtu?“***

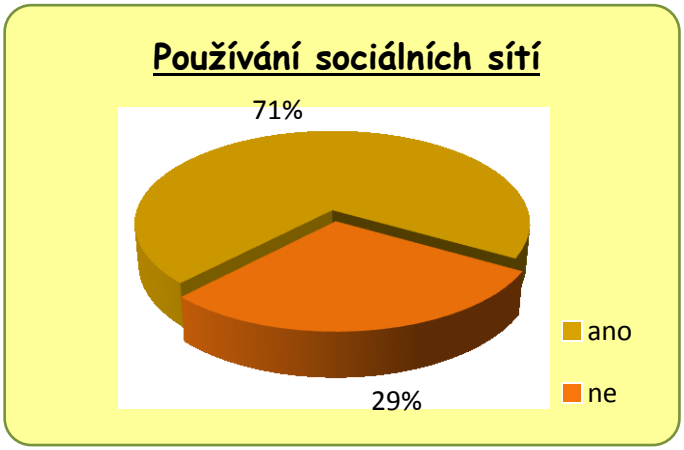
Graf 11 Obavy ze zneužití bankovního účtu

Zdroj: autorka

Z dalšího grafu můžeme, po srovnání s předchozími dvěma grafy, usuzovat, že nemalé procento lidí používá internetové bankovnictví a platební karty i přes strach, který mají ve vztahu ke zneužití svého bankovního účtu. Strach nemá 48 % lidí, 52 % strach ze zneužití má.

12. otázka: ***„Používáte některou ze sociálních sítí?“***

Graf 12 Používání sociálních sítí

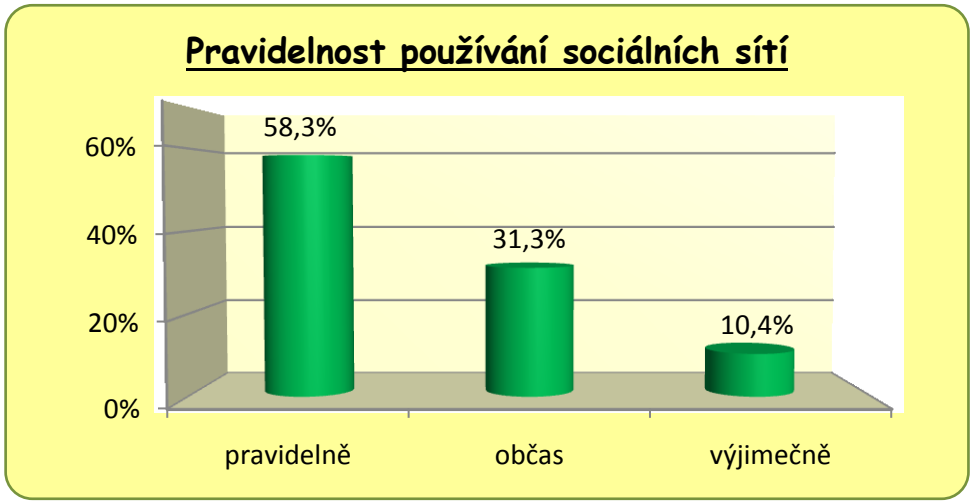


Zdroj: autorka

Četnost v používání sociálních sítí mezi dotazovanými nebyla překvapující. Dnešní doba se sociálními sítěmi vyznačuje a dá se říct, že je jakýmsi soudobým fenoménem. V průzkumu odpovědělo na otázku používání sociálních sítí kladně 71 % lidí, 29 % dotázaných sociální sítě nepoužívá.

13. otázka: ***„Jak často používáte sociální síť?“***

Graf 13 Pravidelnost používání sociálních sítí

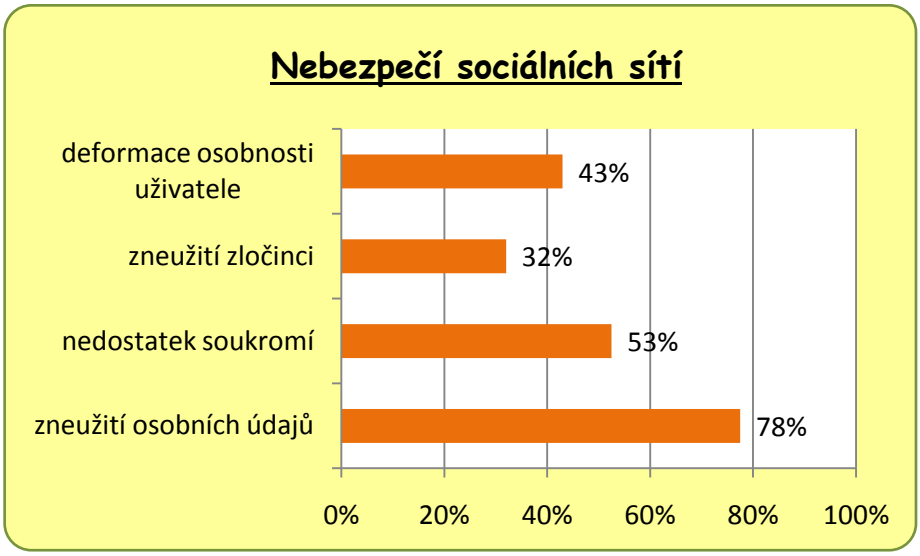


Zdroj: autorka

Z lidí, kteří používají sociální sítě, je navštěvuje pravidelně 58,3 % dotazovaných, 31,3 % je v kontaktu se sociálními sítěmi občas a výjimečně jen 10,4 %.

14. otázka: ***„Jaká nebezpečí spatřujete v sociálních sítích?“***

Graf 14 Nebezpečí sociálních sítí



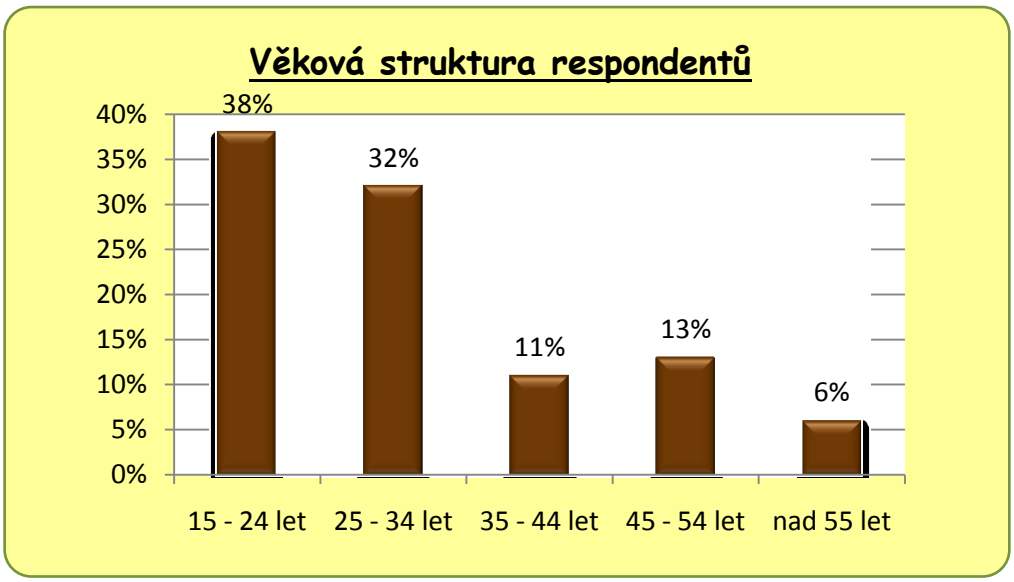
Zdroj: autorka

Další otázka byla zaměřena na nebezpečí, jaké respondenti spatřují v sociálních sítích. Ze zneužití sociálních sítí má strach 78 % z celého vzorku dotazovaných. 53 % vidí problém v nedostatku soukromí a 43 % je znepokojeno určitou možnou deformací

osobnosti uživatelů. Nejmenší, i když stejně dosti podstatný díl, konkrétně 32 % respondentů má strach ze zneužití sociálních sítí zločinci.

15. otázka: ***„Jaký je Váš věk?“***

Graf 15 Věková struktura respondentů

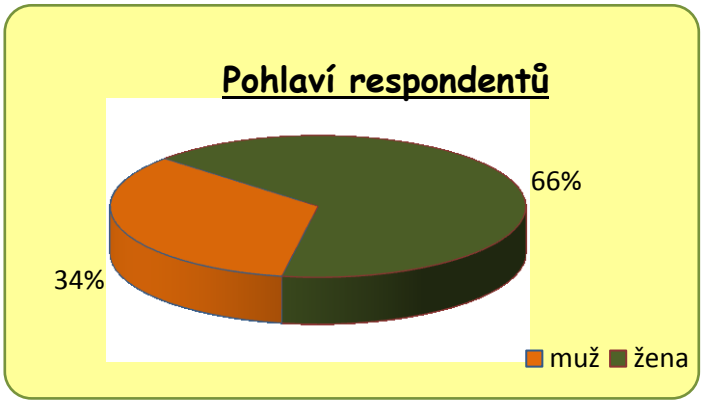


Zdroj: autorka

Z grafu 15 Věková struktura respondentů můžeme vidět, že největší procentuální zastoupení mají lidé ve věku 15 – 24 let (38 %). Hned po nich následuje skupina lidí ve věku 25 – 34 let (32 %). Nejmenší procento respondentů bylo zastoupeno ve věkové kategorii nad 55 let a to v počtu 6 % z celkových 200 dotázaných.

16. otázka: ***„Jste žena/muž?“***

Graf 16 Pohlaví respondentů



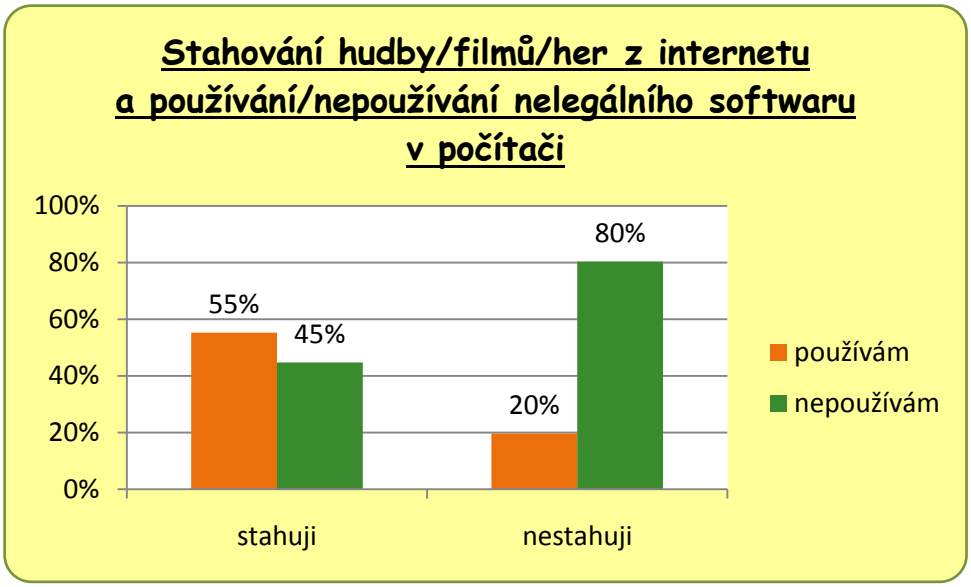
Zdroj: autorka

Z celkového počtu 200 dotázaných respondentů bylo 34 % mužů a 66 % žen.

Kombinované grafy a vyhodnocení

1. ***Graf***

Graf 17 Stahování hudby/filmů/her z internetu a používání/nepoužívání nelegálního softwaru v počítači

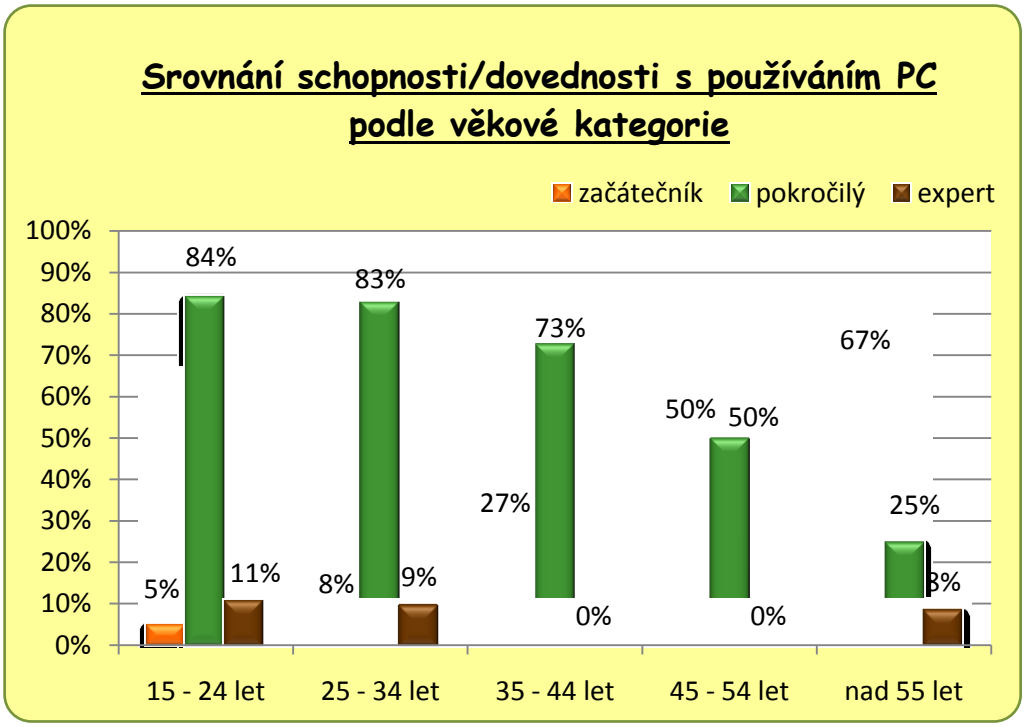


Zdroj: autorka

Ze srovnání počtů lidí, kteří stahují nebo nestahují hudbu, filmy a hry z internetu, a lidí, kteří používají, resp. nepoužívají nelegální software, vidíme jasnou souvislost. 80 % respondentů ze skupiny lidí, kteří nestahují z internetu výše uvedené produkty, nepoužívá ani nelegální software. Ve skupině lidí, kteří produkty stahují, je situace v používání nelegálního software v podstatě vyrovnaná. 55 % používá nelegální software a 45 % ne. Bylo by určitě zajímavé provést pro porovnání podobné srovnání za několik let.

2. *Graf*

Graf 18 Srovnání schopnosti/dovednosti s používáním PC podle věkové kategorie

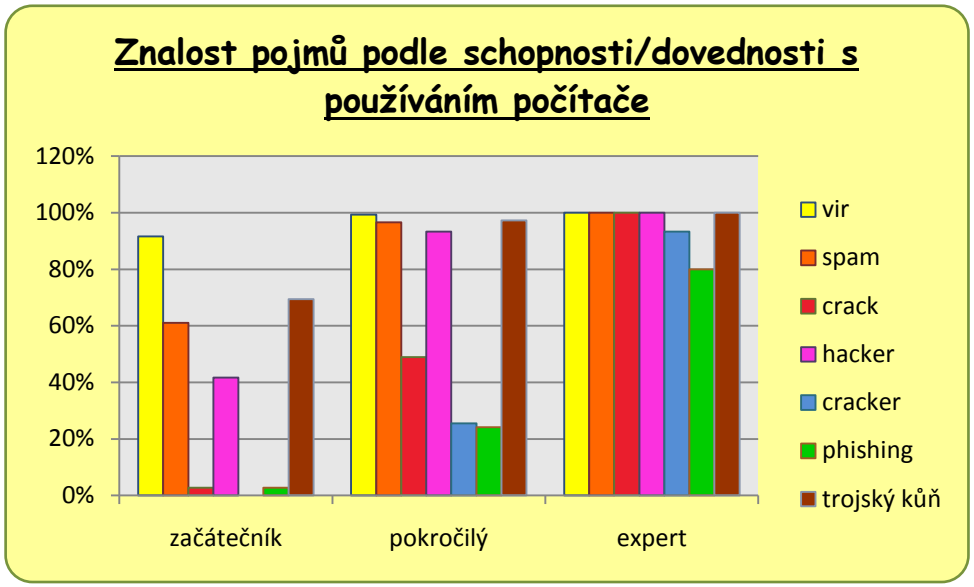


Zdroj: autorka

Srovnání schopností s používáním počítače podle věku více či méně potvrdilo společenský názor, podle kterého jsou starší lidí počítačově méně gramotní. Je zajímavé, že v nejstarší věkové kategorii se jako expert označilo srovnatelné množství respondentů jako v prvních dvou věkových skupinách. Toto hodnocení je však značně subjektivní, je tedy možné, že vysoké hodnocení vlastních schopností u starších lidí je ovlivněno menším rozhledem v oblasti schopností a funkcí dnešních počítačů.

3. *Graf*

Graf 19 Znalost pojmů podle schopnosti/dovednosti s používáním počítače

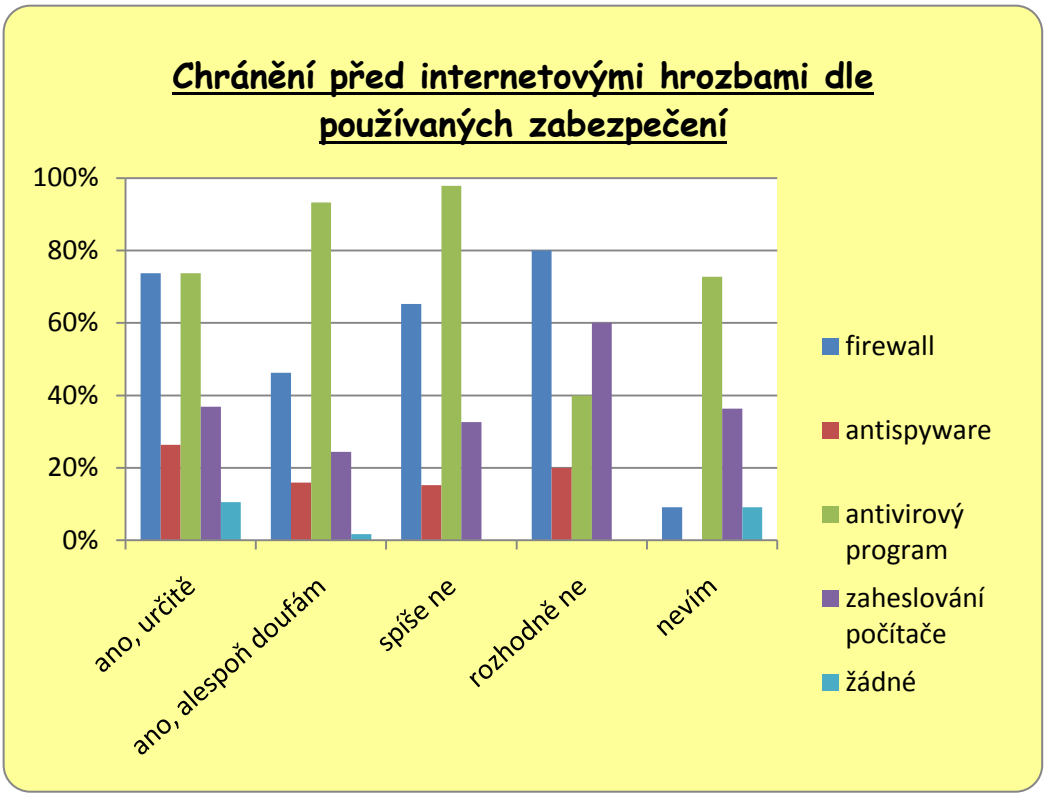


Zdroj: autorka

Z tohoto grafu vyplývá, že lidé své schopnosti označovali vesměs objektivně, i když se jistě mohly vyskytnout některé výjimky, které z tohoto pohledu nemůžeme rozeznat. Zajímavé je, že *phishing* jako známý pojem, označilo nejmenší procento lidí. Pravděpodobně to vypovídá o nedostatečné informovanosti o internetových hrozbách v rámci prevence a hlavně nedostatku pozornosti respondentů, neboť právě tento pojem je často zmiňován v rámci informací o internetových bankovních podvodech.

4. *Graf*

Graf 20 Chránění před internetovými hrozbami dle používaných zabezpečení

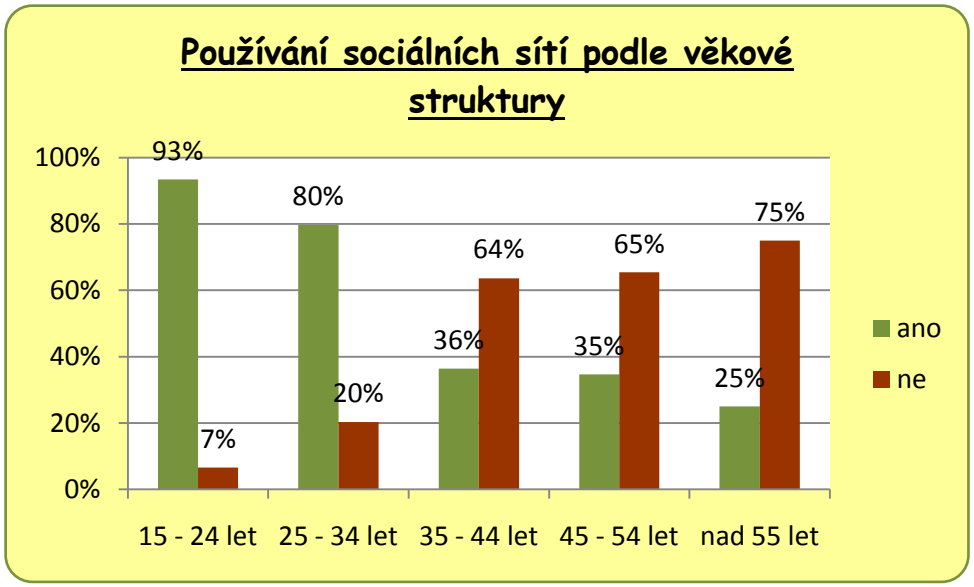


Zdroj: autorka

Pohledem do tohoto grafu zjistíme, že lidé jsou, co se týče hodnocení bezpečnosti svého počítače, velmi sebejistí. Např. pouze ¾ lidí z těch, co si jsou svým zabezpečením jistí, používají antivirový program. Zajímavostí je, že firewall, který je součástí všech novějších operačních systému firmy Microsoft, není uživateli počítačů používán. Existuje také možnost, že lidé firewall neoznačili, neboť přesně nevěděli, o jakou součást ochrany počítače se jedná.

5. *Graf*

Graf 21 Používání sociálních sítí podle věkové struktury

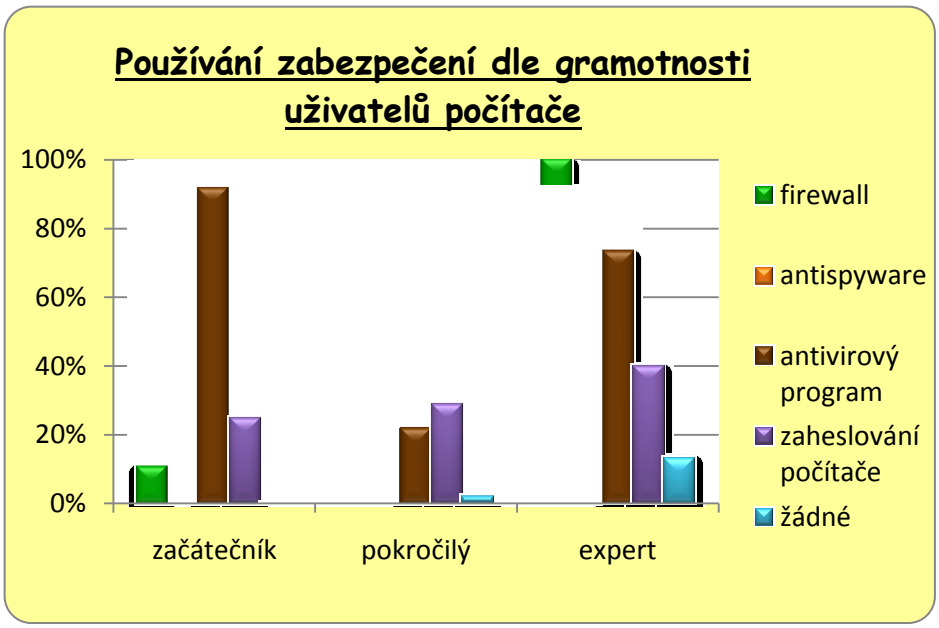


Zdroj: autorka

Hodnoty tohoto grafu jenom potvrzují trend posledních několika let, kdy jsou životy mladé generace v podstatě spjaty se sociálními sítěmi, a vidíme, že lidé používají intenzivně sociální sítě i v druhé věkové kategorii. Co se týká dalších věkových skupin, mezi nimi je oblíbenost sociálních sítí již o poznání menší.

6. *Graf*

Graf 22 Používání zabezpečení dle gramotnosti uživatelů počítače



Zdroj: autorka

V porovnání gramotnosti uživatelů a úrovně zabezpečení jejich počítačů si můžeme všimnout několika zajímavostí. Antivirový program používají v největší míře začátečníci, kteří však již v podstatě žádné další zabezpečení nepoužívají. Naproti tomu lidé označující se jako experti používají podle všeho komplexnější ochranu, avšak již samotné nepoužití antivirového programu v asi 30% případů je zarážející.

4.3 Shrnutí příčin vyplývajících z výzkumu

Podle všeho je zásadním problémem flegmatičnost a negramotnost lidí ve vztahu k počítačové kriminalitě a jejich domýšlivost v tom, že mají za to, že počítače ovládají, ale přitom nerespektují základní bezpečnostní pravidla. Jak bychom si mohli jinak vysvětlit, že lidé, kteří se označují jako experti, pokud se týká používání počítačových technologií, používají antivirový program jen asi v 70 % případů. A proč se v této skupině vyskytují respondenti, kteří nepoužívají žádné zabezpečení. Dokonce si můžeme povšimnout, že začátečníci používají antivirové programy v největší míře ze všech skupin dotazovaných. Z toho se dá usuzovat, že lidé ze skupiny začátečníků vědí jen o jediné ochraně, kterou je právě antivirové zabezpečení.

V médiích se často mluví o zločinech a útocích hackerů na banky či úřady vládních institucí po celém světě, ale pojmy, v nich používané jsou nesprávné. Ve spojení se závislostí lidí na médiích je i toto brzdícím článkem v celém procesu jakési prevence, která by měla spočívat především ve snahách obeznámit lidi s nebezpečím internetu a moderních technologií. Je třeba říci, že technologie nejsou jenom zábava, ale že se dnes v jejich prostředích žijí i celé životy, a proto by se k nim tak mělo přistupovat.

Dalším problémem je nemožnost naprosté dokonalosti složitých aplikací jako operačních systémů. Stará jádra operačních systémů nebyla programována na boj s dnešními typy útoků, a tak se i přes značné úsilí nedaří tyto chyby odstraňovat. Čas od času objeví díra v zabezpečení důležité aplikace nebo aktualizace a vzniká riziko napadení.

4.4 Důsledky počítačové kriminality

4.4.1 Ekonomické důsledky

Kriminalita je něčím, co má negativní dopad na celou společnost. Způsobuje nejen materiální škody, ale také narušuje morální hodnoty takovým způsobem, že je důležité proti ní zasáhnout. V prostředí počítačů by si jejich uživatelé měli uvědomit, že stačí jedno kliknutí myši a mohou se stát obětí počítačové kriminality. Nyní popíši některé důsledky počítačové kriminality, kterých je velké množství.

Podle zdrojů, které poskytly tajné služby Spojených států, se stále více pachatelů zaměřuje spíše na malé a střední podniky[71], kterým schází prostředky pro kvalitní zabezpečení jejich počítačů. Hlavními příčinami nedostatečného zabezpečení počítačů a komunikační infrastruktury je malý rozsah financování a mylná domněnka, že pachatelé se o tyto menší firmy nezajímají a útoky na ně jsou nepravděpodobné. Proto tyto podniky nemají dostatečně vypracované plány na řešení počítačových útoků. Naproti tomu jsou zde velké a bohaté firmy, které do zabezpečení svých systémů investují nemalé prostředky a tyto mohou útokům lépe vzdorovat. Navíc se při jejich napadení útočník vystavuje poměrně velkému riziku odhalení a tedy i riziku dopadení.[72]

Důsledky softwarového pirátství

Globální krize, která postihla ekonomický a finanční sektor, zapříčinila vznik nového jevu. Není jím nic jiného než rostoucí počet udání za používání nelegálního softwaru. Růst počtu těchto případů je způsoben ve velké míře tím, že zaměstnavatelé jsou častěji nuceni propouštět své zaměstnance a někteří z těchto zaměstnanců pak mají tendenci se mstít. Nejjednodušším způsobem, jak svému bývalému zaměstnavateli způsobit velké potíže, je nahlášení používání softwarového vybavení, ke kterému daná společnost nevlastní příslušnou licenci.

V dřívějších dobách bylo počítačové pirátství doménou jednotlivců, kteří si softwarové vybavení stahovali pro svou potřebu. Dnes existují organizované gangy, které

[71] Malý firmy zaměstnávají do 50 zaměstnanců, střední firmy od 50 do 249 zaměstnanců a velké firmy od 250 zaměstnanců

[72] Novinky.cz. *Hackeři se zaměřují na menší firmy, které nemají peníze na ochranu počítačů.* [online]. 15. 9. 2009. [cit. 27. 02. 2011]. Dostupný z WWW: <http://www.novinky.cz/internet-a-pc/software/179070-hackeri-se-zameruji-na-mensi-firmy-ktere-nemaji-penize-na-ochranu-pocitacu.html>.

pirátský software distribuují, prodávají a vydělávají tak obrovské peníze. Obvyklou praktikou těchto skupin je nalákat, většinou nezkušeného, uživatele počítače na koupi oblíbených programů. Většinou se jedná o operační systémy a kancelářské balíky firmy Microsoft, grafické editory firmy Adobe a počítačové hry. Zmíněné programy pak nabízejí se slevou až 90 % oproti legální verzi na falešných internetových obchodech, takže poctivý kupující nemusí poznat, že se jedná o nelegální kopie. Zákazník po nákupu v mnohých případech vlastní nejen pirátskou kopii softwaru, ale pirátskou kopii doplněnou o škodlivý kód, který může útočníkům sloužit jako zadní vrátka k ovládnutí systému, získání přístupu k bankovním účtům a osobním údajům.

Mluvčí BSA Jan Hlaváček uvedl, že v případě pořízení a následném používání nelegálního softwaru, hrozí pachatelům pirátství finanční postih zpravidla ve výši dvojnásobku ceny legálního softwaru, který musí uhradit výrobcům, jimž vznikla škoda, aniž kupující věděl či nevěděl o pořízení nelegálního softwaru. Dále hrozí propadnutí věci nebo dokonce odnětí svobody až na dobu pěti let.

Protipirátská organizace BSA 28. ledna 2011 uvedla: „S*oftwarové pirátství v tuzemských firmách je na ústupu. Loni podíl nelegálních programů klesl o tři procentní body na zhruba třicet procent. V domácnostech naopak softwarové pirátství roste a podíl programů bez zaplacené licence je už poloviční.*[73]

Klesající tendence podílu používání nelegálního softwaru ve firmách je způsobena především tím, že manažeři a majitelé firem mají obavy z následků porušení zákona, který znamená záznam v trestním rejstříku.

Vysoký podíl nelegálního softwaru v celkovém množství softwaru používaného v domácnostech, je zapříčiněn snadnou dostupností pirátského softwaru na Internetu, kde uživatelé požadovaný software snadno najdou a případně i zakoupí.

Protože údaje týkající se používání pirátských kopií softwaru v roce 2010 budou dostupné až v květnu letošního roku, uvádím pro představu v Příloze č. 6 tabulku míry pirátství v jednotlivých státech Evropské unie za období 2007 až 2009.

[73] Finanční noviny. *Softwarové pirátství ve firmách loni kleslo, v domácnostech roste.* [online]. 28. 1. 2011. [cit. 21. 02. 2011]. Dostupný z WWW: <http://www.financninoviny.cz/zpravy/softwarove-piratstvi-ve-firmach-loni-kleslo-v-domacnostech-roste/588102>.

V tabulce je vidět, že Česká republika se v roce 2009 umístila na jedenácté příčce ze sedmadvaceti členských zemí Evropské unie a celosvětově byla na dvaadvacátém místě. Ve spojených státech či v Japonsku nebo na Novém Zélandu se softwarové pirátství vyskytuje nejméně (kolem 20 %). Naopak nejvíce nelegálního užívání softwaru je v asijských a afrických rozvojových zemích (přes 90 %).

Pro zajímavost ještě uvádím nejčastější výmluvy softwarových pirátů podle analýzy BSA 2010:[74]

Výmluvy softwarových pirátu podle analýzy BSA 2010
1. Za software nezodpovídám
Za legálnost softwaru zodpovídá někdo jiný, zejména správce sítě.
2. O užívání nelegálního softwaru jsem vůbec nevěděl
Často zaznívá ve snaze zbavit se odpovědnosti.
3. Na hlídání softwaru nemám čas
Máme jiné priority související přímo s podnikáním a licence neřeším.
4. Licence jsme zrovna chtěli nakoupit
Protože naše firma roste příliš rychle či došlo k fúzi nebo akvizici a zatím jsme se k narovnání licencí nedostali.
5. Software jsme pouze testovali a pak jej zapomněli odinstalovat
Typická výmluva patřící mezi nejméně uvěřitelné. Je obvykle doprovázena argumentem, že přece není možné mít software stoprocentně pod kontrolou.
6. To mi nainstaloval kamarád, já tomu vůbec nerozumím
Populární argument domácích pirátů. Uvěřitelné pouze v případě, že jde o staršího uživatele nebo pokud byl nelegální software nainstalován při nákupu počítače.

[74] Business Software Alliance. *Za nelegální software v roce 2011 firmy zaplatí 260 tisíc korun.* [online]. 31. 1. 2011 [cit. 28.02.2011]. Dostupný z WWW: <http://www.itpoint.cz/zprava/?i=za-nelegalni-software-v-roce-2011-firmy-zaplati-260-tisic-korun-6540>.

Důsledky kriminality na Internetu

Existuje mnoho výrobců bezpečnostního softwaru, kteří umožňují počítačovým uživatelům bezpečně procházet Internetem a bezpečně vyhledávat či nakupovat. Jedním z těchto výrobců je společnost Symantec, která má k pro tento účel panel nástrojů Norton Safe Web Lite.

Podle studie společnosti, uveřejněné 8. září 2010, došlo k obrovskému rozmachu počítačové kriminality. *„Více než třetina nejpopulárnějších hledaných termínů vykázala nejméně 10 % nebezpečných výsledků, které vystavují počítače a osobní údaje uživatelů riziku, že se stanou obětí počítačové kriminality.“*[75] Riziko spočívá v automatickém stahování z Internetu, které může zapříčinit infikování počítače.

V roce 2010 firma zaznamenala neuvěřitelných 286 milionů odlišných hrozeb, což bylo v průměru 9 nových hrozeb každou vteřinu, které jsou cílené na domácnosti, firemní a vládní počítače.

Tato alarmující čísla se odrážejí i v osobním životě obětí, která se cítí podvedená, rozzlobená, má pocit hněvu a přesto nemá chuť učinit něco pro svou vlastní ochranu. Více než polovina obětí případ počítačové kriminality ani neohlásí. Jak uvedl Joseph LaBrie, PhD, mimořádný profesor psychologie na Loyola Marymount University: *„Je to, jako když vás okradou v autoservisu. Pokud nevíte dost o autech, nebudete se s automechanikem hádat. Lidé se prostě smíří se situací, i když z toho nemají dobrý pocit.“*

Je pochopitelné, že lidem, kteří se stali obětí této kriminality, může být nepříjemné vyšetřování, které může trvat i déle než měsíc. Ale měli bychom si uvědomit, že pokud škodu nenahlásíme, můžeme tak pachateli nepřímo napomoci k tomu, že nebude postihnut za tento trestný čin a může svou kriminální činnost spokojeně provádět dál. Výrobce antivirového softwaru AVG uvedl, že si kyberzločinci mohou takhle přijít na částku až 200 000 korun denně.[76]

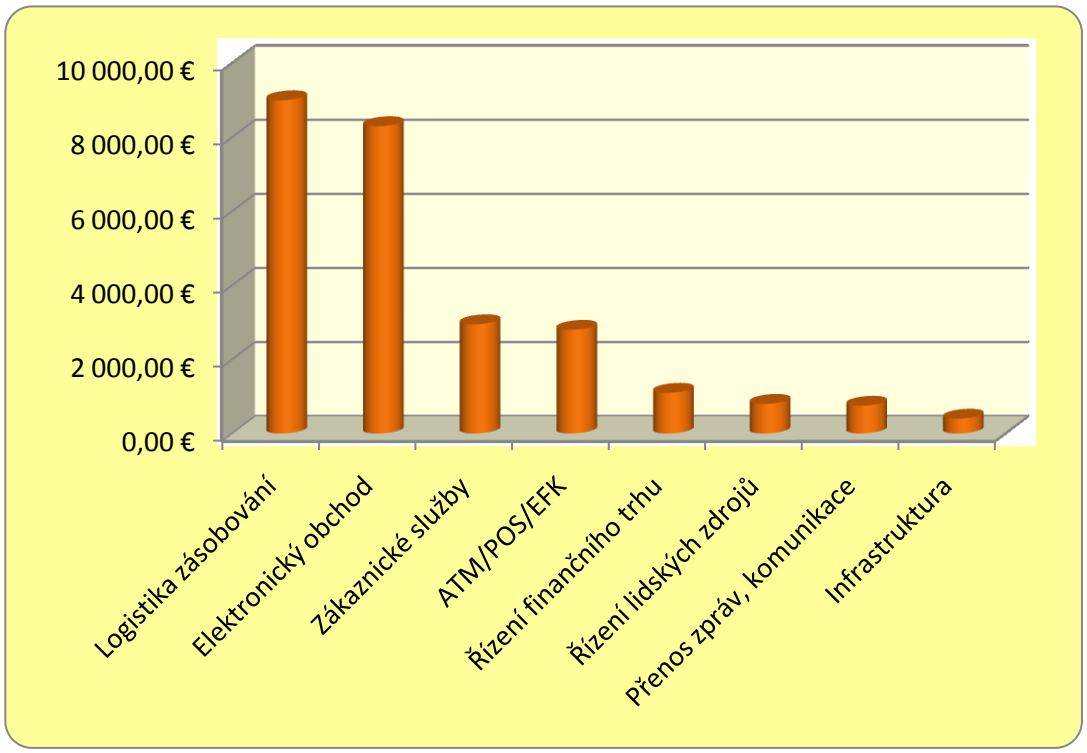
V následujícím grafu je ukázáno, jaké ztráty za jednu minutu mohou způsobit výpadky informačních systémů zapříčiněné kybernetickými útoky. Jsou dělené podle typických segmentů trhu, ve kterých se informační systémy nejvíce uplatňují.

---

[75] Business Software Alliance. *Za nelegální software v roce 2011 firmy zaplatí 260 tisíc korun.* [online]. 31. 1. 2011 [cit. 28.02.2011]. Dostupný z WWW: <http://www.itpoint.cz/zprava/?i=za-nelegalni-software-v-roce-2011-firmy-zaplati-260-tisic-korun-6540>.

[76] Mediafax.cz. *Počítačová kriminalita stále roste, kyberzločinci vydělávají až 200 tisíc korun denně.* [online]. 23. 2. 2011 [cit. 28.02.2011]. Dostupný z WWW: <http://www.mediafax.cz/ekonomika/3177043-Pocitacova-kriminalita-stale-roste-kyberzlocinci-vydelavaji-az-200-tisic-korun-denne>.

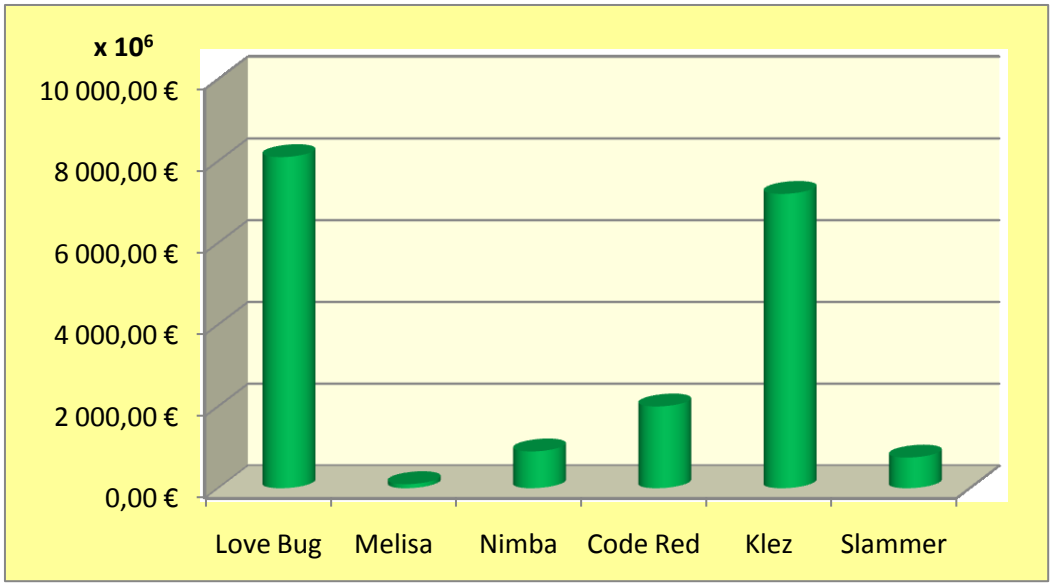
Obrázek 6 Ztráty za minutu výpadku informačního systému



Zdroj: Jirovský,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 131

V dalším grafu jsou ukázány škody v milionech eur způsobené nejznámějšími a nejzákeřnějšími typy malwaru.

Obrázek 7: Způsobené ztráty (podle typu malware)



Zdroj: Jirovský,V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. První vydání, Praha 2007. Grada Publishing, a.s. 288 s. ISBN 978-80-247-1561-2. Str. 104

4.4.2 Právní důsledky

Obrovským nedostatkem při řešení trestné činnosti počítačové kriminality je nízký počet odborníků zabývajících se touto problematikou. Tento stav má za následek to, že většina případů, spadajících do oblasti počítačové kriminality, zůstane nevyřešena a pachatelé tak velmi snadno uniknou spravedlivému trestu.

Počet případů počítačové kriminality stále roste a prodloužená doba soudních řízení a nedostatečný počet odborníků v řadách policie je velkým problémem. Podle vedoucího oddělení informační kriminality Policejního prezidia ČR Karla Kuchaříka trvá dlouhou dobu, než se policie k případům dostane a poté jsou informace o trestné činnosti a samotných pachatelích a důkazy, kterých je mnohdy dostatek, neprokazatelné a celý případ se musí odložit.

Z důvodu nízkého počtu příslušníků policie, kteří by byli zároveň odborníky na počítačovou kriminalitu, si policie musí vybírat případy nejzásadnější a ty, které ohrožují zdraví a životy lidí. A to i přesto, že zákon nařizuje, že musí být řešena veškerá trestná činnost.

Do funkce policejního odborníka mohou nastoupit pouze policisti, kteří mají odslouženo minimálně devět let ve sboru a jsou schopnými počítačovými experty. Podle Kuchaříka by stačilo, kdyby měl člověk odsloužen jeden rok u policie a byl by, po zaškolení, přijat, ovšem tohle zákon neumožňuje.[77]

Dalším problémem týkajícím se právních důsledků kyberkriminality je, že se legislativa v oblasti počítačové kriminality vyvíjí pomaleji než dění v kyberprostoru a velká část úředníků a státních činitelů si to neuvědomuje a pro nápravu nic nedělají. Chybí zde dostatečná právní úprava a Česká republika patří mezi země, kde pro Internet či počítačové hry neplatí skoro žádná omezení. Jak uvedl docent Jírovský: *„Bránit se zatím moc neumíme, vyhráváme jen včerejší bitvy“*. Podle něj se snažíme modifikovat zákony staré i stovky let tak, aby postihovaly něco, co existuje jen chvíli.[78] Z toho vyplývá, že by bylo pravděpodobně účinnější vymyslet úplně nové zákony, které by se přizpůsobily dnešnímu dění a chování společnosti.

---

[77] Novinky.cz. *Policie nestíhá šetřit počítačovou kriminalitu.* [online]. 24. 5. 2010 [cit. 28.02.2011]. Dostupný z WWW: <http://www.novinky.cz/krimi/201056-policie-nestiha-setrit-pocitacovou-kriminalitu.html>.

[78] Cesnet. *Hrozba kyberterorismu roste.* [online]. 27. 6. 2010 [cit. 01.03.2011]. Dostupný z WWW: <http://www.cesnet.cz/sdruzeni/napsali-o-nas/2010/06/20100627_Lupa.html>.

4.4.3 Technické důsledky

Jako hlavní důsledek počítačové kriminality je přinejmenším to, že se díky ní počítačové technologie vyvíjejí mnohem rychleji, než kdyby k žádnému boji v kyberprostoru nedocházelo. Asi nejcitelněji firmy bojují proti porušování autorských práv a to jak u softwarových produktů, tak u hudebních či video souborů. Největší a nejsilnější společnosti světa se spojují, aby čelily tomuto problému společnými silami.

Minulost nám ukazuje, že možnost ochrany počítačového softwaru proti nelegálnímu šíření je značně omezená především z důvodu velkého množství uživatelů, kdy stačí několik málo jednotlivců, kteří ochranu nějakým způsobem překonají a v podstatě ihned je na Internetu dostupný postup nebo program, který pomůže ochranu prolomit i ostatním. Na druhou stranu si musíme uvědomit, že co se týče softwarových výrobků pro dnešní herní konzole, tak zde se situace mění v tom, že k použití nelegální kopie je obvykle nutný zásah přímo do zařízení, čímž je nejen porušena dohoda, která danému výrobku zabezpečuje záruční lhůtu, ale chybný zásah může celé zařízení i úplně zničit.

Pokud se vrátíme zpět ke klasickým počítačům, není bez zajímavosti, že firma Intel na začátku tohoto roku představila svůj systém, který již hardwarově nebude umožňovat kopírování a šíření souborů s mediálním obsahem. Systém funguje na principu zákazu přenosu obsahu přes nezabezpečené kanály uvnitř PC.[79]

Co se týká boje s pirátstvím na softwarové úrovni, můžeme zmínit například nástroj Genuine firmy Microsoft, která pomocí něho zjistí o svých produktech nainstalovaných na počítači, zda jsou legální. Pokud program zjistí, že nainstalovaný software legální není, zamezí například stahování aktualizací, které jsou dnes více než kdy jindy důležité pro bezpečný chod počítače, nebo začne uživatele obtěžovat zobrazováním textů týkajících se zakoupení originálního výrobku.

Vývoj zaznamenala také oblast autentizace a autentifikace, kdy je u důležitých systémů nahrazeno jednoduché přihlášení přes login a heslo dalšími doplňujícími atributy (kód zaslaný pomocí SMS apod.). V neposlední řadě se již ve velké míře používá zabezpečení pomocí biometrických údajů jako jsou otisky prstů, tvar obličeje, vlastnosti oka nebo styl chůze.[80]

[79] Wired. *Intel BeefsUp CPUs With Graphics Power – and Content Protection.* [online]. 5. 1. 2011 [cit. 06.03.2011]. Dostupný z WWW: <http://www.wired.com/gadgetlab/2011/01/intel-cpu/>.
[80] Access server. *Autentizační metody založené na biometrických informacích.* [online]. 18. 11. 2010 [cit. 06.03.2011]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>.

5 Opatření proti páchání počítačové kriminality

Řešením počítačové kriminality se dnes musí zabývat všechny státy i firmy, které ke svému podnikání potřebují moderní technologie. Najít prostředky ve světe informačních technologií, které by mohly potlačit negativní důsledky pokroku je velmi těžké, ne-li nemožné. Existuje však několik pravidel, které mohou dopady počítačové kriminality alespoň snížit.

U všech druhů kriminality se mluví o důležitosti prevence a není tomu jinak ani u té počítačové. Od jiných druhů prevence se však liší tím, jak je řešena.

5.1 Znalosti

Jednou z možných způsobů prevence, které se samy nabízejí, je rozšíření dostatečného množství znalostí mezi uživatele počítačů tak, aby jejich chování neumožňovalo počítačovým zločincům snadný útok. Pokud si uvědomíme, že lidé ani neznají základní prvky, kterými se v prostředí počítačů chránit a v podstatě nevnímají nebezpečí, které jim hrozí, pak musíme konstatovat, že je zde velký prostor pro nápravu. V médiích můžeme často slyšet o útocích hackerů na informační centra vyspělých států či bankovní systémy, nebo o tom, jak lidé mění nápisy na elektronických cedulích dálnic. Všechny tři zmíněné případy spadají do kategorie, která uživatele neznepokojí a mnohdy ho spíše pobaví.

Proto je nutné lidem nějakým způsobem naléhavě sdělit, v čem přesně tkví nebezpečí počítačové kriminality a že i oni se mohou stát jejími cíli. Je třeba jim vysvětlit, čím jsou ohroženi právě oni jako jedinci nebo rodiny, aby jim stálo za to, starat se o svůj život v kyberprostoru alespoň stejně dobře jako o svůj život fyzický. Uživatel musí vědět, jaké způsoby podvodníci používají k tomu, aby své oběti oklamali a naučit se je rozpoznat a bojovat proti nim.

V dnešní době nemůžeme čekat, že lidé, jejichž věk přesáhl určitou hranici, budou rozumět způsobu života, jaký žijí mladší generace, ale zůstává pravdou, že alespoň základní návyky týkající se chování v kyberprostoru, by nějakým způsobem získat měli. Tito lidé často pracují na počítačích i v kancelářích firem, a proto by se těmto firmám určitě vyplatilo školení svých zaměstnanců nejen v bezpečnosti práce apod., ale také v bezpečnosti práce na internetu, aby se dozvěděli proč aktualizovat software a jak to

provádět, v čem je nebezpečí pirátství softwaru apod. Potom je zde šance, že si zaměstnanec přenese návyky pracovní i domů a bude se podle nich chovat.

Co se týká generací mladších, je nejjednodušším způsobem řešení návyků upravením výuky ve školách tak, aby byli žáci donuceni s počítačem pracovat a aby již v mládí pochopili, že počítač a internet by měl být především nástrojem pracovním a až poté prostředkem zábavy. Pokud budou počítač používat k práci, o kterou nechtějí přijít, pak se budou snažit o to, aby jejich počítače byly maximálně zabezpečeny tak, aby o svá data a zároveň pracovně strávené hodiny nemuseli mít strach.

5.2 Investice

Z jednoho z předchozích zhodnocení vyplynulo, že velké množství lidí stále využívá nelegální software a stahují hudbu, videa a hry z internetu. Osobně si však myslím, že tak, jako investujeme do nového auta a jeho servisu, tak bychom měli investovat i do počítače a jeho vybavení, pokud jej využíváme. Je velmi snadno odvoditelné, že používáním nelegálního softwaru vzniká velké riziko napadení útočníkem, neboť nelegální kopie programu může obsahovat další programy, o kterých uživatel nemá ani tušení. Tato situace však u zaručeně originální kopie nastat nemůže.

Dalším problémem pirátských kopií, především u nejpoužívanějších operačních systémů firmy Microsoft, je to, že neumožňují, popř. znesnadňují stahování aktualizací, které se často týkají právě bezpečnosti. Toto chování je způsobeno tím, že u některých aktualizací je nutné zároveň spustit ověření právě aktualizovaného systému pomocí nástroje, který je schopen nelegální kopii odhalit a uživatele pak pravidelně upozorňovat na to, že používá pirátský software. Z tohoto důvodu velké množství uživatelů vypíná automatickou instalaci aktualizací a to zvětšuje bezpečnostní riziko.

Tyto dva důvody jsou dostačující k tomu, aby jednotlivci i firmy investovaly do softwarového vybavení dostatečné prostředky, popř. se rozhodli pro používání bezplatných aplikací.

Dalšími produkty, které jsou častým cílem pirátství, jsou počítačové hry. U nich nehrozí ani tak nebezpečí napadení za pomoci upravené originální aplikace, ale pro jejich správný chod bez použití originálního digitálního média je obvykle nutno použít tzv. crack. Crack je program, který většinou pracuje tak, že vymazáním originálního licenčního čísla z jádra aplikace umožní použití veřejně dostupného klíče. Pokud je však takový program napsán zkušeným odborníkem na počítačové technologie a ještě je o něm známo, že se

dopouští napomáhání k počítačové kriminalitě, jak si můžeme být jistí, že se nezaměřuje ještě na něco jiného? Sám crack tedy může být škodlivým kódem a většina správně nastavených a aktualizovaných antivirových programů, pokud mají možnost crack zkontrolovat, nalezne škodlivý kód, který buď vychází ze samotné funkce cracku a nemusí tedy znamenat nic nebezpečného nebo se o nebezpečný kód opravdu jedná. Téměř nikdy nemůžeme mít jistotu, která z těchto dvou možností je ta správná.

Proto bych doporučila v co největší míře propagovat originální software a eliminací nebezpečí, vyplývajících z používání pirátských kopií softwaru.

5.3 Použití svobodného softwaru

Používání svobodného softwaru je frekventovaným tématem ve vztahu k počítačové kriminalitě. Z operačních systémů, které tvoří základ softwarového vybavení počítače, je znám, jako svobodný produkt, operační systém Linux. Ten má oproti operačním systémům Windows některé zásadní nevýhody. V prvé řadě na jeho používání lidé nejsou zvyklí díky rozšířenosti operačních systémů firmy Microsoft a výrobci hardwaru pro něj neposkytují dostatečnou podporu v podobě ovladačů a i dostupných softwarových výrobků kompatibilních s Linuxem je menší počet. Má však také jednu, a to dosti zásadní, výhodu oproti konkurenčním produktům. Jeho zkonstruován tak, že sám o sobě velmi dobře odolává počítačovým útokům a proto nepotřebuje ani žádný složitý zabezpečovací systém. Také obvyklé útočné nástroje ve formě virů apod. nebudou na systému Linux fungovat, protože jsou tyto nebezpečné kódy napsány obvykle v programovacím jazyce, který OS Linux sám o sobě nepodporuje. Pokud člověk používá počítač pouze k práci, pak je schopen tento operační systém vyhovět všem jeho požadavkům, protože jeho součástí je jak kancelářský balík Open Office, tak internetový prohlížeč, IM (instant messenger). Programátorům nabízí možnost instalace všech potřebných pracovních nástrojů.

5.4 Solidarita-ceny

Nyní bych se ráda podívala na druhou stranu pirátství, která je sice sporná, ale přesto možná. Při dnešních cenách softwaru je docela pochopitelné, že lidé raději riskují pirátstvím, než aby si daný produkt zakoupili. Je otázkou, do jaké míry by míra pirátství na počítačovém softwaru klesla, kdyby se ceny produktů skokově snížily. Možnou cestu ve změně systému cen počítačového softwaru bych viděla i v tom, že by si uživatel software „předplatil“ na několik let dopředu, takže by si nemusel každé tři roky kupovat

nový operační systém nebo grafické studio. Není samozřejmě podmínkou používat stále nejmodernější software, ale pokud ho člověk využívá k práci, pak je to nanejvýš vhodné, neboť se postupně mění systémy ovládání a vzhled a člověk by nemusel větší skoky zvládat v tom, že by se v novém softwaru neorientoval. Podle mého názoru by mohly velké firmy, zabývající se formou softwaru, více zužitkovat své znalosti a know-how a organizovat různá placená školení jiných specialistů, nebo vydělávat spíše na profesionální podpoře produktů. Některé podobné systémy financování firem samozřejmě již fungují, avšak asi ne v takové míře, jak by si obyčejný uživatel přál.

Podobný způsob boje s pirátstvím vidím i u děl hudebních. Tady si myslím, že by měli autoři a umělci více vydělávat na nadstandardním materiálu, jakým mohou být videa z natáčení alb a práce ve studiu, vydávání demo nahrávek a nevydaných skladeb. Dnešní technika umožňuje návštěvníkům koncertů koupit si záznam ze zmíněné akce již při odchodu z koncertu. Mám za to, že skalní fanoušci, a nejen ti, by možnosti využili a produkty by si ve velké míře kupovali. Jde jen o to rozšířit sortiment zboží a praktikovat nové nápady s tím, aby zaujaly co největší počet zákazníků a posluchačů, kteří by o produkty daného umělce měli zájem.

Uvědomuji si, že to, co člověk chce, měl by si i zaplatit, ale pokud existují jiné cesty k tomu, aby byl spokojený jak výrobce, tak zákazník-uživatel, potom stojí za to tyto cesty vyzkoušet.

5.5 Aktuální opatření proti počítačovým útokům

Mezi aktuální opatření, která chce Evropská komise do dvou let zřídit, je založení centra EU pro boj s počítačovou kriminalitou a vytvoření systému pro varování a sdílení informací, který by měl zvýšit bezpečnost v kyberprostoru. Opatření patří mezi 5 hlavních cílů[81] zamýšlené Strategie vnitřní bezpečnosti Evropské unie. Komise uvedla, že by centrum mělo pomoci vytvořit větší kapacity pro vyšetřování počítačové trestné činnosti a mělo by být jakýmsi prostředníkem mezi vnitrostátními skupinami pro reakci na počítačové hrozby. [82]

[81] boj proti organizovanému zločinu, terorismu, počítačové trestné činnosti, krizím a katastrofám

[82] Novinky.cz. *Evropská komise chce založit centrum pro boj s počítačovou kriminalitou.* [online]. 24. 2. 2011 [cit. 02.03.2011]. Dostupný z WWW: <http://www.novinky.cz/internet-a-pc/226089-evropska-komise-chce-zalozit-centrum-pro-boj-s-pocitacovou-kriminalitou.html>.

Proti počítačovým útokům se od 1.1.2011 snaží bojovat také bezpečnostní tým „Computer Security Incident Response Team“ České republiky (dále jen „CSIRT.CZ„). Od 3. dubna 2008 díky šestimiliónovému grantu od Ministerstva vnitra pod projektovým názvem CSIRT.CZ pracovali odborníci Univerzity Karlovy a ČVUT s experty ze sdružení CESNET, CZ.NIC a informační společnosti Ness na včasném odhalení počítačových útoků. Letos tříletý grant ministerstva vypršel a sdružení CESNET a CZ.NIC se dohodly, že sdružení CZ.NIC tento tým povede.

Národní tým CSIRT.CZ se má podílet na efektivním řešení vzniklých incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice a dle možnosti jim předcházet. Při řešení bude shromažďovat a vyhodnocovat data o oznámených incidentech a předávat hlášené incidenty osobám zodpovědným za chod sítě, která je zdrojem daného incidentu. CSIRT.CZ není určena jako „help-line“ pro běžného uživatele, ale poskytuje koordinační pomoc při řešení incidentů.[83]

[83] Ministerstvo vnitra České republiky. *Memorandum o Computer Security Incident Response Team České republiky.* [cit. 02.03.2011]. Dostupný z WWW: <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

6 Závěr

Rozvoj informačních technologií a počet odvětví jejich praktického využívání mají strmě vzestupnou tendenci. Informační technologie dnes nejsou doménou pouze technologických odvětví, ale jsou hojně využívány ve školství, státní správě či bankovnictví. Obchody, restaurace, benzínové stanice i relaxační a sportovní centra jsou na informačních technologiích přímo závislé. Všechna tato odvětví používají počítače a telekomunikace pro provádění bankovních operací, včetně plateb zákazníků, nebo shromažďování mnohdy citlivých informací.

S rostoucím počtem možností provádění těchto základních operací, které se v dnešní době dotýkají většiny lidí, rostou také možnosti zločinců využívat nové technologie, postupy a znalosti ve svůj prospěch. S rozvojem technologie je tedy třeba rozvíjet i její zabezpečení.

Z důvodu nadčasovosti problémů informačních a komunikačních technologií jsem si vybrala jako téma diplomové práce právě počítačovou kriminalitu, její příčiny a dopady na lidskou společnost.

Pokud chceme porozumět současné podobě počítačové kriminality, musíme porozumět historii, jejíž počátky se datují v sedmdesátých letech dvacátého století. Popsání a vysvětlení historického vývoje kriminality v kyberprostoru a jejího právního ošetření v minulosti jsem se věnovala v úvodu práce. Navázala jsem rozdělením počítačové kriminality a jejích pachatelů.

Další část jsem věnovala zkoumání příčin a důsledků vzniku počítačové kriminality a její nebezpečnosti. Pro lepší pochopení jsem provedla průzkum návyků uživatelů počítačů a vyhodnocením jsem získala názornější náhled na některé příčiny kybernetické kriminality. Popsáním ekonomických, právních a technických důsledků jsem tento okruh ukončila.

Nakonec jsem navrhla některá opatření, která by mohla zlepšit bezpečnostní situaci v kyberprostoru a dalších oblastech, které se ho dotýkají. Uvedla jsem též aktuální opatření, která jsou proti počítačové kriminalitě v prostředí moderních technologií zavedena.

Na závěr bych chtěla zmínit myšlenku pana europoslance T. Kelama, který srovnává počítačový útok s útokem jaderné hlavice. Říká o nich: *„V případě útoku raketou s jadernou hlavicí, máte minuty, dokonce až půl hodiny na ověření zprávy. V případě počítačového útoku, musíte jednat okamžitě, v milisekundách.“*. Z toho vyplývá, že

nebezpečí počítačové kriminality se dotýká každého z nás a nemůžeme ho ignorovat. Musíme proti ní bojovat všemi dostupnými prostředky a se stejným úsilím jako u všech ostatních druhů kriminality.

Seznam použité literatury

Monografické zdroje:

[1] GERLOCH, A. *Teorie práva*. 5. vyd. Plzeň: Aleš Čeněk, 2009. 308 s. ISBN 978-80-7380-233-2.

[2] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo.* 1. vydání Praha 2008. Auditorium. 220 s. ISBN 978-80-903786-7-4.

[3] HARVÁNEK, J. a kolektiv. *Teorie práva*. Plzeň: Aleš Čeněk, 2008. 501 s. ISBN 978-80-7380-104-5.

[4] JELÍNEK, J. a kolektiv. *Obecná část . Trestní právo hmotné.* 1. vydání, Praha 2004. Linde Praha, a.s. 470 s. ISBN 80-7201-501-X.

[5] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada Publishing, a. s., 2007. 288 s. ISBN 978-80-247-1561-2.

[6] KNAPP, V., *Teorie práva*. 1.vyd. Praha: C.H.Beck, 1995. 247 s. ISBN 80-7179-028-1.

[7] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vyd. Brno: Computer Press, 2002. 120 s. ISBN 80-7226-419-4.

[8] SMEJKAL, V. *Internet a §§§.* 2. aktualit. a rozš. vyd. Praha: Grada Publishing, 2001. 284 s. ISBN 80-247-0058-1.

[9] SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systému.* 1. vydání. Praha: C. H. Beck, 2001. 542 s. ISBN 80-7179-552-6.

[10] SZOR,P. *Počítačové viry analýza útoku a obrana*. 1 vyd. Praha: Zoner Press 2006. 608s. ISBN 80-86815-04-8.

Právní předpisy:

[11] Zákon č. 40/2009 Sb., Trestní zákoník

[12] Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů

Elektronické zdroje:

[13] Access server. *Autentizační metody založené na biometrických informacích.* [online]. 18. 11. 2010 [cit. 06.03.2011]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>.

[14] Business center.cz. *Právní norma.* [online]. [cit. 13.02.2011]. Dostupný z WWW: <http://business.center.cz/business/pojmy/p707-pravni-norma.aspx>.

[15] Business Software Alliance. *Co je softwarové pirátství?* [online]. [cit. 21.02.2011]. Dostupný z WWW: <http://www.bsa.org/country.aspx>.

[16] Business Software Alliance. *Za nelegální software v roce 2011 firmy zaplatí 260 tisíc korun.* [online]. 31. 1. 2011 [cit. 28.02.2011]. Dostupný z WWW: <http://www.itpoint.cz/zprava/?i=za-nelegalni-software-v-roce-2011-firmy-zaplati-260-tisic-korun-6540>.

[17] ČINČERA, J. *Mha přede mnou, mha za mnou - hoaxes útočí na lidskou solidaritu*. Ikaros elektronický časopis o informační společnosti. 2002, roč. 6, č. 4 [online]. [cit. 15.02.2011]. Dostupný z WWW: < http://www.ikaros.cz/node/931>. ISSN 1212-5075.

[18] Diit. *Kauza Minoret tajemství zbavená.* [online]. 29. 1. 2003 [cit. 15.02.2011]. Dostupný z WWW: < http://www.diit.cz/clanek/kauza-mironet-tajemstvi-zbavena/4541/>.

[19] Findarticles. *Business Publications.* [online]. 23. 3. 1996 [cit. 23.01.2011]. Dostupný z WWW: < http://findarticles.com/p/articles/mi_m0EKF/is_n2109_v42/ai_18135525/>.

[20] Hoax. *Phishing.* [online]. 3. 1. 2011 [cit. 14.02.2011]. Dostupný z WWW: <http://www.hoax.cz/phishing/internetove-bankovnictvi-rb-20110104/>.

[21] KRATOCHVÍL, P. *Nejnovější triky internetových zlodějů.* CHIP elektronický časopis o počítačích a digitální technice. 2010, č. 4 [online]. [cit. 15.02.2011]. Dostupný z WWW: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2010/chip-06-2010/nej-triky.>.

[22] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení* [cit. 15.02.2011]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>.

[23] Ministerstvo vnitra České republiky. *Memorandum o Computer Security Incident Response Team České republiky.* [cit. 02.03.2011]. Dostupný z WWW: <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

[24] Právní rádce. *Postih počítačové kriminality podle nového trestního zákona.* [online]. 22. 7. 2009 [cit. 08.03.2011]. Dostupný z WWW: <

http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

[25] Radiožurnál. Český rozhlas 1. *Představuje internet nebezpečí.* [online]. 27. 1. 2009 [cit. 01.03.2011]. Dostupný z WWW: <http://zpravy.rozhlas.cz/radiozurnal/podkuzi/_zprava/540206>.

[26] Sagit: Nakladatelství ekonomické a právní literatury Ostrava. *Objektivní a subjektivní právo* [online]. 1. 5. 2004 [cit. 13.02.2011]. Dostupný z WWW: <http://www.sagit.cz/pages/lexikonheslatxt.asp?cd=151&typ=r&refresh=yes&levelid=oc_212.htm>.

[27] Sborník z mezinárodní konference. *Bezpečnost v podmínkách organizací a institucí ČR.* [online]. 20. 5. 2005 [cit. 25.02.2011]. Dostupný z WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/sbornik.pdf>.

[28] Symantec. *Norton Safe Web Lite identifikuje rizikové webové stránky.* [online]. 3. 8. 2010 [cit. 28.02.2011]. Dostupný z WWW: <http://www.itpoint.cz/zprava/?i=norton-safe-web-lite-identifikuje-rizikove-webove-stranky-5817>.

[29] Theroxor. *The Awesome size of the internet infographic.* [online]. 28. 10. 2010 [cit. 15.03.2011]. Dostupný z WWW: <http://theroxor.com/2010/10/28/the-awesome-size-of-the-internet-infographic/>.

[30] Wikipedie: Otevřená encyklopedie. *Napster* [online]. 2. 9. 2010 [cit. 23.01.2011]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Napster>.

[31] Wikipedie: Otevřená encyklopedie. *Pornografie* [online]. 25. 1. 2011 [cit. 17.02.2011]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Pornografie>.

[32] Wikipedie: Otevřená encyklopedie. *Cyberstalking* [online]. 28. 2. 2011 [cit. 06.03.2011]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Cyberstalking>.

[33] Wikipedie: Otevřená encyklopedie. *Peer to peer* [online]. 11. 2. 2011 [cit. 15.02.2011]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Peer-to-peer>.

[34] Zákony online. [online]. [cit. 14.02.2011]. Dostupný z WWW: <http://zakony-online.cz/>.

[35] Zlínský deník. *Obtěžování přes internet řeší policie a počítačoví experti.* [online]. 7. 2. 2011 [cit. 06.03.2011]. Dostupný z WWW: <http://zlinsky.denik.cz/zpravy_region/obtezovani-pres-internet-resi-policie-a-pocitacovi.html>.

Seznam zkratek a symbolů

AMD	Advanced Micro Devices
BBS	Bulletin Board System
BSA	Business Software Alliance
CD	Compact Disk (kompaktní disk)
CD-ROM	Compact Disk Read-Only Memory (disk určený pro čtení)
ČNB	Česká národní banka
ČVUT	České vysoké učení technické
DoS	Denial of Service (odmítnutí služby)
DVD	Digital Video Disc (digitální optický datový nosič)
EFF	Electronic Frontier Foundation (Nadace elektronického pohraničí)
EU	Evropská unie
FBI	Federal Bureau of Investigation (Federální úřad pro vyšetřování)
FCIC	Federal Computer Investigations Committee (Federální výbor pro počítačové vyšetřování)
FTP	File Transfer Protocol
ICT	Information and Communication Technologies (informační a komunikační technologie)
IT	Information Technology (informační technologie)
kB	kilobyte
MS	Microsof
PC	Personal Computer (osobní počítač)
SMS	Short message service (služba krátkých zpráv)
TB	Terabyte (1073741824 kB)
TZ	Trestní zákoník
USA	United States of America (Spojené státy americké)
USD	United States dollar (americký dolar)
WWW	World Wide Web (celosvětová síť)

Seznam grafů

Seznam tabulek

Seznam obrázků

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl(a) seznámen(a) s tím, že na mou diplomovou (bakalářskou) práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že jeden výtisk diplomové (bakalářské) práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……

……
jméno a příjmení

studenta

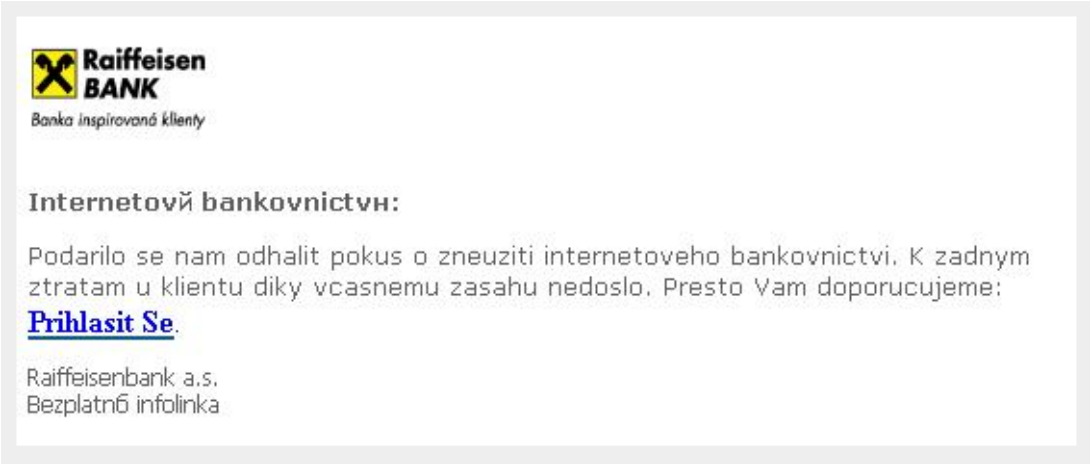
Adresa trvalého pobytu studenta:

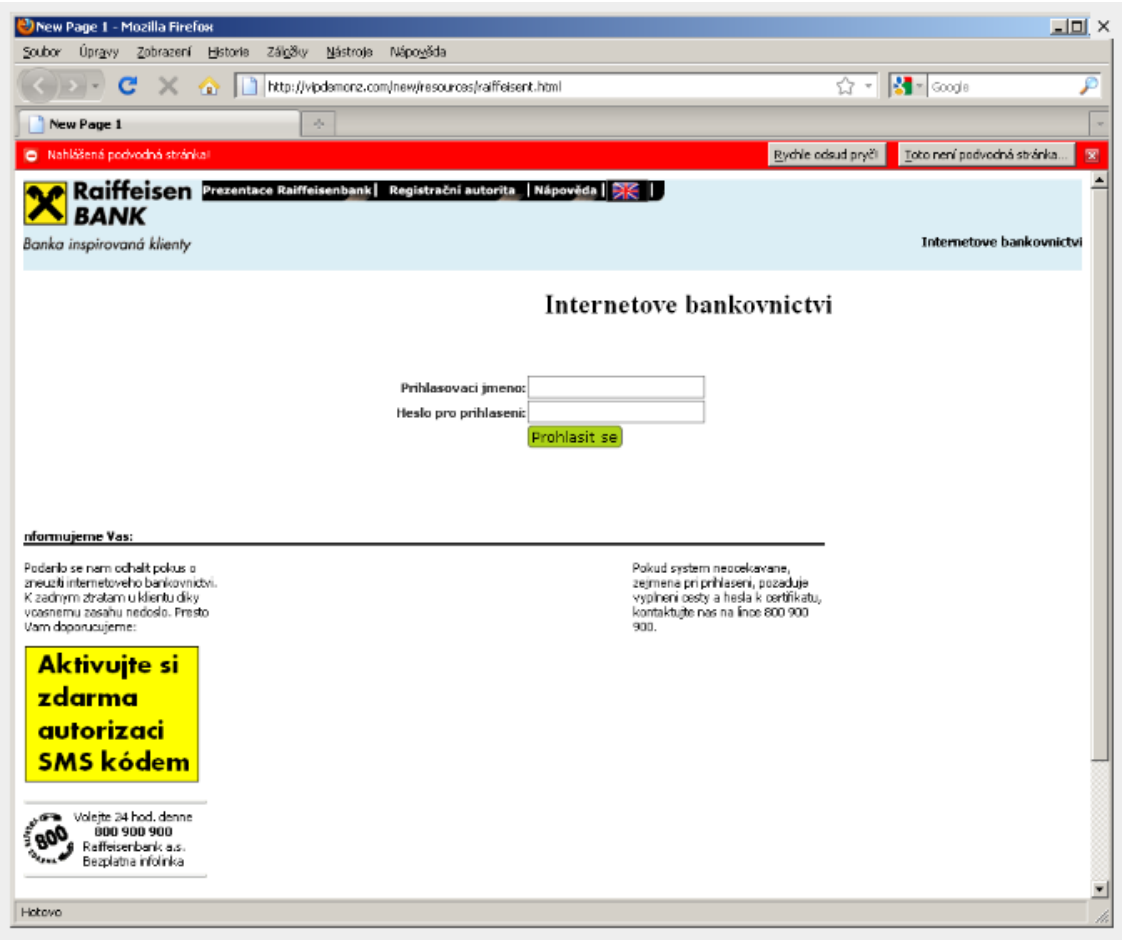
……

Seznam příloh

Příloha č. 1

Ukázka phishingového útoku





Zdroj: Lupa.cz. *Phishingový útok na Raiffeisenbank*. [online]. 11. 1. 2011 [cit. 05.03.2011]. Dostupný z WWW: < http://www.lupa.cz/clanky/phishingovy-utok-na-raiffeisenbank-najde-se-jeste-nejaky-hlupak/>

Příloha č. 2

Ustanovení trestního zákona

Část druhá

Hlava pátá: *Trestné činy proti majetku*

§ 230
Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému
systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 231
Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 232
Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,

a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Příloha č. 3

§ 175 Vydírání

(1) Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.

(2) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin nejméně se dvěma osobami,

c) spáchá-li takový čin se zbraní,

d) způsobí-li takovým činem značnou škodu,

e) spáchá-li takový čin na svědkovi, znalci nebo tlumočníkovi v souvislosti s výkonem jejich povinnosti, nebo

f) spáchá-li takový čin na jiném pro jeho skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je skutečně nebo domněle bez vyznání.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,

a) způsobí-li takovým činem těžkou újmu na zdraví,

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312), nebo

c) způsobí-li takovým činem škodu velkého rozsahu.

(4) Odnětím svobody na osm až šestnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.

(5) Příprava je trestná.

§ 180 Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

(3) Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo

b) takového tajemství využije.

(3) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin ze zavrženíhodné pohnutky,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako úřední osoba,

b) způsobí-li takovým činem škodu velkého rozsahu, nebo

c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

(5) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který

a) spáchá čin uvedený v odstavci 1 nebo 2,

b) jinému úmyslně umožní spáchat takový čin, nebo

c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem,

bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.

(6) Odnětím svobody na tři léta až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 5 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 184 Pomluva

(1) Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.

(2) Odnětím svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

§ 191 Šíření pornografie

(1) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo

a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo

b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny,

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 206 Zpronevěra

(1) Kdo si přisvojí cizí věc nebo jinou majetkovou hodnotu, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

d) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.

§ 207 Neoprávněné užívání cizí věci

(1) Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu je přechodně užívat, nebo
kdo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takové věci, které mu byly svěřeny, přechodně užívá,
bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

b) spáchá-li takový čin jako člen organizované skupiny, nebo

c) způsobí-li takovým činem značnou škodu.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

§ 209 Podvod

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

d) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.

§ 213 Provozování nepoctivých her a sázek

(1) Kdo provozuje peněžní nebo jinou podobnou hru nebo sázku, jejíž pravidla nezaručují rovné možnosti výhry všem účastníkům, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 větší škodu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného větší prospěch.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu, nebo

c) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 228 Poškození cizí věci

(1) Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Stejně bude potrestán, kdo poškodí cizí věc tím, že ji postříká, pomaluje či popíše barvou nebo jinou látkou.

(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 na věci svědka, znalce nebo tlumočníka pro výkon jejich povinnosti,

b) spáchá-li takový čin na věci jiného pro jeho skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je skutečně nebo domněle bez vyznání,

c) spáchá-li takový čin na věci, která požívá ochrany podle jiného právního předpisu, nebo

d) způsobí-li takovým činem značnou škodu.

(4) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu.

§ 254 Zkreslování údajů o stavu hospodaření a jmění

(1) Kdo nevede účetní knihy, zápisy nebo jiné doklady sloužící k přehledu o stavu hospodaření a majetku nebo k jejich kontrole, ač je k tomu podle zákona povinen, kdo v takových účetních knihách, zápisech nebo jiných dokladech uvede nepravdivé nebo hrubě zkreslené údaje, nebo kdo takové účetní knihy, zápisy nebo jiné doklady změní, zničí, poškodí, učiní neupotřebitelnými nebo zatají, a ohrozí tak majetková práva jiného nebo včasné a řádné vyměření daně, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo uvede nepravdivé nebo hrubě zkreslené údaje v podkladech sloužících pro zápis do obchodního rejstříku, nadačního rejstříku, rejstříku obecně prospěšných společností nebo rejstříku společenství vlastníků jednotek anebo v takových podkladech zamlčí podstatné skutečnosti, kdo v podkladech sloužících pro vypracování znaleckého posudku, který se přikládá k návrhu na zápis do obchodního rejstříku, nadačního rejstříku, rejstříku obecně prospěšných společností nebo rejstříku společenství vlastníků jednotek uvede nepravdivé nebohrubě zkreslené údaje nebo v takových podkladech zamlčí podstatné údaje, nebo kdo jiného ohrozí nebo omezí na právech tím, že bez zbytečného odkladu nepodá návrh na zápis zákonem stanoveného údaje do obchodního rejstříku, nadačního rejstříku, rejstříku obecně prospěšných společností nebo rejstříku

společenství vlastníků jednotek nebo neuloží listinu do sbírky listin, ač je k tomu podle zákona nebo smlouvy povinen.
(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 na cizím majetku značnou škodu.
(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 na cizím majetku škodu velkého rozsahu.

§ 268 Porušení práv k ochranné známce a jiným označením

(1) Kdo uvede do oběhu výrobky nebo poskytuje služby neoprávněně označené ochrannou známkou, k níž přísluší výhradní právo jinému, nebo známkou s ní zaměnitelnou nebo pro tento účel sobě nebo jinému takové výrobky nabízí, zprostředkuje, vyrobí, doveze, vyveze nebo jinak opatří nebo přechovává, anebo takovou službu nabídne nebo zprostředkuje, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Stejně bude potrestán, kdo pro dosažení hospodářského prospěchu neoprávněně užívá obchodní firmu nebo jakékoliv označení s ní zaměnitelné nebo uvede do oběhu výrobky nebo služby neoprávněně opatřené označením původu nebo zeměpisným označením anebo takovým označením s ním zaměnitelným nebo pro tento účel sobě nebo jinému takové výrobky nebo služby nabídne, zprostředkuje, vyrobí, doveze, vyveze nebo jinak opatří nebo přechovává.
(3) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 nebo 2 pro sebe nebo pro jiného značný prospěch, nebo

b) dopustí-li se takového činu ve značném rozsahu.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 nebo 2 pro sebe nebo pro jiného prospěch velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.

§ 269 Porušení chráněných průmyslových práv

(1) Kdo neoprávněně zasáhne nikoli nepatrně do práv k chráněnému vynálezu, průmyslovému vzoru, užitnému vzoru nebo topografii polovodičového výrobku, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

c) dopustí-li se takového činu ve značném rozsahu.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.

§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.

§ 317 Ohrožení utajované informace

(1) Kdo vyzvídá informaci utajovanou podle jiného právního předpisu s cílem vyzradit ji nepovolané osobě, kdo s takovým cílem sbírá údaje obsahující utajovanou informaci nebo kdo takovou utajovanou informaci nepovolané osobě úmyslně vyzradí, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) vyzradí-li úmyslně nepovolané osobě utajovanou informaci v jiném právním předpisu klasifikovanou stupněm utajení „Přísně tajné“ nebo „Tajné“,

b) spáchá-li čin uvedený v odstavci 1, ačkoli mu ochrana utajovaných informací byla zvlášť uložena, nebo

c) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li značnou škodu nebo jiný zvlášť závažný následek.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,

a) týká-li se čin uvedený v odstavci 1 utajované informace z oblasti zabezpečení obranyschopnosti České republiky klasifikované v jiném právním předpisu stupněm utajení „Přísně tajné“, nebo

b) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu.

(4) Příprava je trestná.

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob

(1) Kdo veřejně hanobí

a) některý národ, jeho jazyk, některou rasu nebo etnickou skupinu, nebo

b) skupinu osob pro jejich skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že jsou skutečně nebo domněle bez vyznání,

bude potrestán odnětím svobody až na dvě léta.

(2) Odnětím svobody až na tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) nejméně se dvěma osobami, nebo

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

(1) Kdo veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků, bude potrestán odnětím svobody až na dvě léta.

(2) Stejně bude potrestán, kdo se spolčí nebo srotí k spáchání činu uvedeného v odstavci 1.

(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

b) účastní-li se aktivně takovým činem činnosti skupiny, organizace nebo sdružení, které hlásá diskriminaci, násilí nebo rasovou, etnickou, třídní, náboženskou nebo jinou nenávist.

§ 357 Šíření poplašné zprávy

(1) Kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Kdo zprávu uvedenou v odstavci 1 nebo jinou nepravdivou zprávu, která je způsobilá vyvolat opatření vedoucí k nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa anebo bezdůvodnou záchrannou práci integrovaného záchranného systému sdělí soudu, orgánu Policie České republiky, orgánu státní správy, územní samosprávy, nebo jinému orgánu veřejné moci, právnické osobě, fyzické osobě, která je podnikatelem, anebo hromadnému informačnímu prostředku, bude potrestán odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 opětovně,

b) spáchá-li takový čin jako člen organizované skupiny,

c) způsobí-li takovým činem značnou škodu,

d) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy soudu nebo jiného orgánu veřejné moci, nebo,

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

b) způsobí-li takovým činem škodu velkého rozsahu.

Příloha č. 4

Srovnání mezi tradičními a počítačovými zločiny

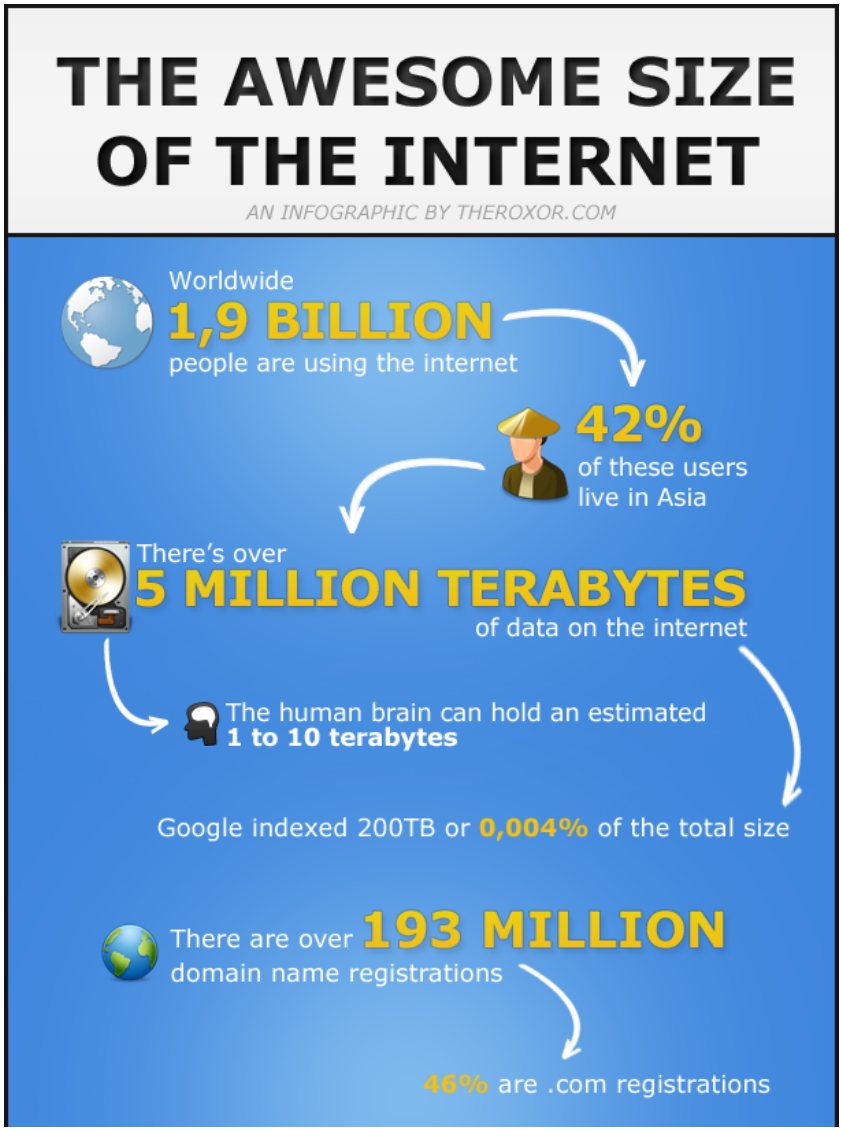
TRADIČNÍ ZLOČINY	POČÍTAČOVÉ ZLOČINY
Bankovní loupež Klasická bankovní loupež, při které gangy vtrhnou a vyloupí banku nebo bezpečnostní dodávku s penězi.	***Nabourání systému*** Nabourání do bankovního systému a převod peněz prostřednictvím elektronických platebních systémů.
Vloupání Falešná návštěva vám zaklepe na dveře a předstírá, že za vámi přišla z nějakého legitimního důvodu. Mezitím se k vám oknem vloupe spolupachatel a ukradne vám váš cenný majetek.	***Trojské viry*** Stejný mechanismus funguje i v síti. Hacker využije okno nebo zadní dvířka, které najde v počítači oběti a tím dovnitř vpustí škodlivý kód, který pro něj následně pracuje.
Výpalné V minulosti organizované zločinecké gangy nutili obchodníky, aby jim platili za „ochranu“, tady za to, že jejich obchody nevykradou nebo nevypálí	***Online vydírání*** Dnes se pokoušejí organizovaní zločinci nutit společnosti podnikající na síti, aby jim zaplatili výkupné za to, že před útokem „ochrání“ jejich elektronické obchody.
Krádež kreditní karty Zločinci kradou výpisy z účtů a stvrzenky, aby mohli podvodně zneužít identitu svých obětí.	***„Vyčmuchání“ čísla kreditní karty*** Počítačoví zločinci do počítače oběti nainstalují programy pro odposlech dat (sniffer), které z klávesnice odečítají hesla a uživatelská jména a posílají je zpět zločinci.
Podvodní telefonisté Zločinci zavolají oběti a pod záminkou, že jsou z banky nebo policie se jí vyptávají na číslo kreditní karty, identifikační čísla nebo hesla.	***Phishing*** Elektronická pošta přesměruje oběť phishingu na webovou stránku zločince, která kopíruje vzhled webové stránky banky. Nic netušící oběť následně zločinci poskytne číslo své bankovní karty, PIN, bezpečnostní údaje a podobně.
Mladí pouliční drogoví dealeři Organizovaní obchodníci s drogami využívají teenagery a děti k dodávkám peněz, zbraní a drog mezi gangy a zákazníky.	***Počítačová dětská práce*** Organizovaní zločinci využívají script kiddies a mladé hackery k tomu, aby jim dodávali a provozovali pro ně webové zbraně v rámci vybírání online výpalného nebo pro realizaci online podvodů.

Kotelnové "investiční podvody" Zločinci si založí falešnou kancelář a předstírají, že jsou akcioví makléři. Přes telefon pak prodávají nevědomým zákazníkům akcie za nadhodnocené ceny, nebo dokonce akcie společností, které se ve skutečnosti na burze vůbec neobchodují.	***Podvody s nadhodnocenými akciemi*** Zločinci nakoupí akcie a za pomocí makléřských webových stránek uměle zkreslí údaje o hodnotě akcií tak, aby je mohli rychle a výhodně prodat.

Zdroj: McAfee. *První celoevropská studie o organizovaném zločinu a internetu.* [online]. 20. 10. 2009 [cit. 01.03.2011]. Dostupný z WWW: <http://skripta.gootik.net/src/SWI/093/sk_kybernalita_McAfee_kriminalita.pdf>

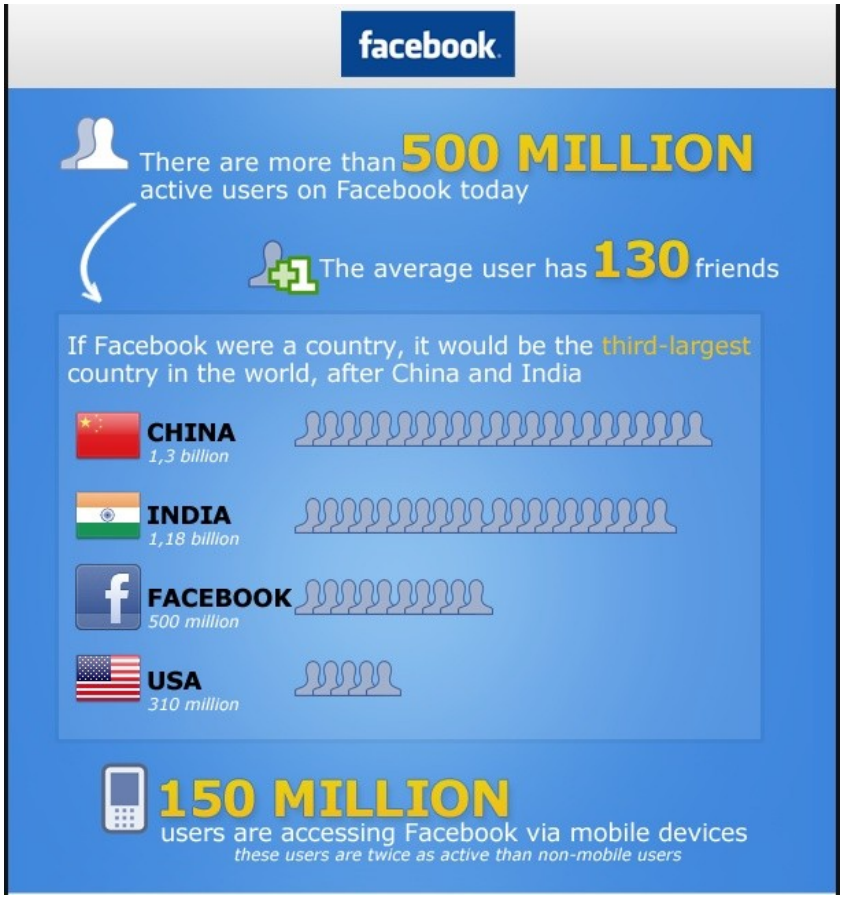
Příloha č. 5

Objem dat na internetu




YouTube
Over 2 BILLION videos are viewed on Youtube each day
24 HOURS of video is uploaded every minute
Top 3 most viewed videos on Youtube:
Justin Bieber ft. Ludacris - Baby
344,194,152 views
Lady Gaga - Bad Romance
287,254,587 views
Charlie bit my finger - again!
234,951,237 views
Every week, the equivalent of
60,000 FULL LENGHTS FILMS
is uploaded to YouTube


twitter
There are over
106 MILLION
Twitter accounts
What's happening?
these users send 55 MILLION tweets per day
That's circa 640 tweets/second
300,000 people join Twitter every day
RERERENCES
http://www.internetworldstats.com/stats.htm
http://www.verisign.com/domain-name-services/domain-information-center/industry-brief/index.html
http://www.facebook.com/press/info.php?statistics
http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/
http://www.socialme.nl/stats/twitter-stats-april-2010/
http://www.website-monitoring.com/blog/2010/05/17/youtube-facts-and-figures-history-statistics/
THEROXOR
because design rocks!



Zdroj: Theroxor. *The Awesome size of the internet infographic.* [online]. 28. 10. 2010 [cit. 15.03.2011]. Dostupný z WWW: <http://theroxor.com/2010/10/28/the-awesome-size-of-the-internet-infographic/>

Příloha č. 6

Míra pirátství v jednotlivých státech Evropské unie

			Míra pirátství			Ztráty v mil. USD	
pořadí	země	rozdíl	**2009**	2008	2007	2009	$M
1.	Lucembursko	0 %	**21 %**	21 %	21 %	$	30
2.	Rakousko	1 %	**25 %**	24 %	25 %	$	212
3.	Belgie	0 %	**25 %**	25 %	25 %	$	239
4.	Finsko	- 1 %	**25 %**	26 %	25 %	$	175
5.	Švédsko	0 %	**25 %**	25 %	25 %	$	304
6.	Dánsko	1 %	26 %	25 %	25 %	$	203
7.	Velká Británie	0 %	**27 %**	27 %	26 %	$	1581
8.	Německo	1 %	**28 %**	27 %	27 %	$	2023
9.	Nizozemsko	0 %	**28 %**	28 %	28 %	$	525
10.	Irsko	1 %	**35 %**	34 %	34 %	$	125
11.	**Česká republika**	**- 1 %**	**37 %**	**38 %**	**39 %**	$	174
12.	Francie	- 1 %	**40 %**	41 %	42 %	$	2544
13.	Portugalsko	- 2 %	**40 %**	42 %	43 %	$	221
14.	Maďarsko	- 1 %	**41 %**	42 %	42 %	$	113
15.	Španělsko	0 %	**42 %**	42 %	43 %	$	1014
16.	Slovensko	0 %	**43 %**	43 %	45 %	$	65
17.	Malta	0 %	**45 %**	45 %	46 %	$	7
18.	Slovinsko	- 1 %	**46 %**	47 %	48 %	$	39
19.	Kypr	- 2 %	**48 %**	50 %	50 %	$	16
20.	Itálie	1 %	**49 %**	48 %	49 %	$	1733
21.	Estonsko	0 %	**50 %**	50 %	51 %	$	19

22.	Litva	0 %	**54 %**	54 %	56 %	$	31
23.	Polsko	- 2 %	**54 %**	56 %	57 %	$	506
24.	Lotyšsko	0 %	**56 %**	56 %	56 %	$	24
25.	Řecko	1 %	**58 %**	57 %	58 %	$	248
26.	Rumunsko	- 1 %	**65 %**	66 %	68 %	$	183
27.	Bulharsko	- 1 %	**67 %**	68 %	68 %	$	115
	Evropská unie		35 %	35 %	35 %	$	12469

Zdroj: Novinky.cz. *Ve firmách je méně kradeného softwaru, přibylo pirátu v domácnostech.* [online]. 12. 5. 2009. [cit. 28. 02. 2011]. Dostupný z WWW: <http://www.novinky.cz/internet-a pc/software/168498-ve-firmach-je-mene-kradeneho-softwaru-pribylo-piratu-v-domacnostech.html>.

Příloha č. 7

DOTAZNÍK

Dobrý den,
jsem studentkou VŠB-TU Ekonomické fakulty a obracím se na Vás s prosbou o vyplnění tohoto dotazníku, který je zaměřen na **návyky, zkušenosti a názory uživatelů PC**. Získané informace jsou anonymní a poslouží výhradně k vypracování mé diplomové práce. Vámi vybrané odpovědi **zakřížkujte**. Vždy je možno vybrat jen **jednu** odpověď, pokud není uvedeno jinak.
Děkuji za Vámi strávený čas a ochotu.

1. Jak byste charakterizoval/a svoji schopnost/dovednost s ovládáním a využíváním počítače v životě?
   - ☐ začátečník
   - ☐ pokročilý
   - ☐ expert

2. Stahujete z internetu hudbu/filmy/hry?
   - ☐ ano
   - ☐ ne

3. Označte pojmy, o kterých můžete říci, že víte, co znamenají:
   - ☐ vir
   - ☐ spam
   - ☐ crack
   - ☐ hacker
   - ☐ cracker
   - ☐ phishing
   - ☐ trojský kůň

4. Používáte ve svém počítači nelegální software?
   - ☐ ano
   - ☐ ne

5. Myslíte si, že jste dostatečně chránění proti internetovým hrozbám?
   - ☐ ano, určitě
   - ☐ ano, alespoň doufám
   - ☐ spíše ne
   - ☐ rozhodně ne
   - ☐ nevím

6. Jaký zdroj považujete za největší hrozbu pro váš počítač?
   - ☐ neznámé emaily
   - ☐ stránky s pornografickým materiálem
   - ☐ nelegální software + crack
   - ☐ aplikace a operační systémy s bezpečnostními nedostatky

7. Které z následujících zabezpečení používáte?
   - ☐ Firewall
   - ☐ Antispyware
   - ☐ antivirový program
   - ☐ zaheslování počítače
   - ☐ žádné

8. Jaký antivirový program používáte?
   - ☐ Kaspersky
   - ☐ AVG
   - ☐ MS Security Essentials
   - ☐ Avast
   - ☐ Eset
   - ☐ Panda
   - ☐ F-secure
   - ☐ jiný

9. Platíte platebními kartami přes internet?
   ☐ ano ☐ ne

10. Používáte internetové bankovnictví?
    ☐ ano ☐ ne

11. Máte strach ze zneužití vašeho bankovního účtu?
    ☐ ano ☐ ne

12. Používáte některou ze sociálních sítí?
    - ☐ ano
    - ☐ ne (přejděte, prosím, na otázku č. 14)

13. Jak často používáte sociální síť?
    - ☐ pravidelně
    - ☐ občas
    - ☐ výjimečně

14. Jaká nebezpečí spatřujete v sociálních sítích?(možno označit více odpovědí)
    - ☐ zneužití osobních údajů
    - ☐ nedostatek soukromí
    - ☐ zneužití zločinci
    - ☐ deformace osobnosti uživatele

15. Věk:

☐ 15 – 24 let ☐ 25 – 34 let ☐ 35 – 44 let ☐ 45 – 54 let ☐ 55 – 64 let ☐ nad 65 let

16. Pohlaví:
    ☐ muž ☐ žena